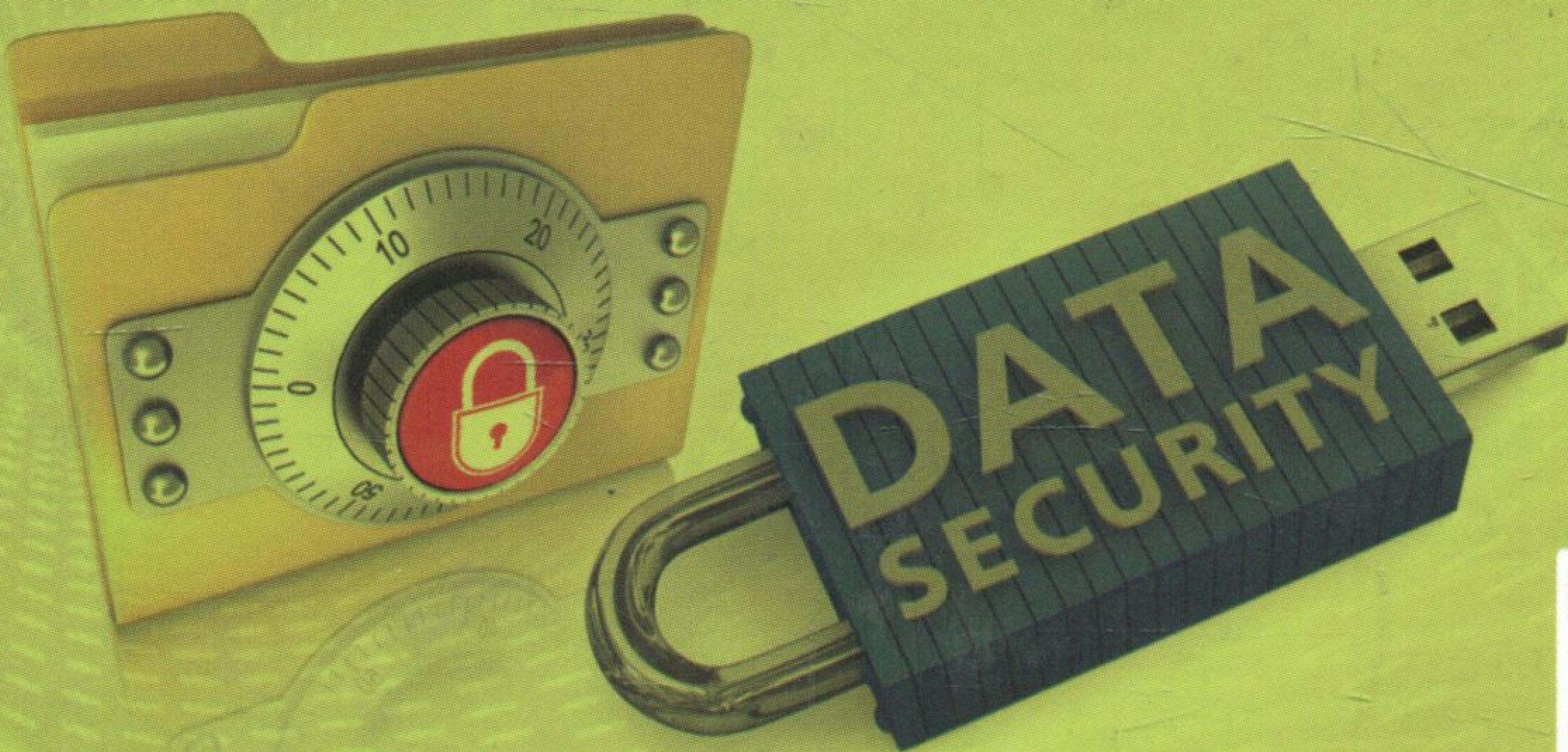
إدارة أمن المعلومات

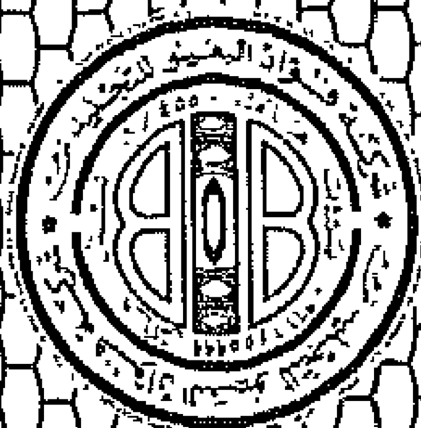
الأستاذ الدكتور
محمد عبد حسين الطائي
كلية الاقتصاد والعلوم الإدارية
جامعة الزرقاء

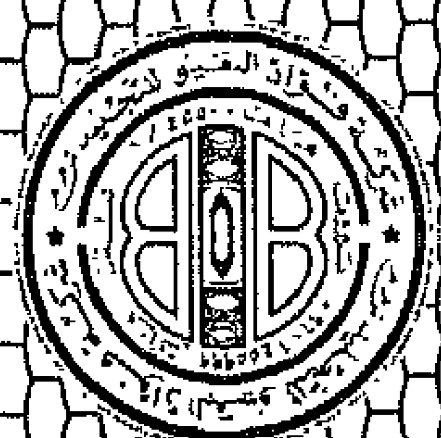
الدكتور
ينال محمود الكيلاني
كلية العلوم الإدارية والمالية
جامعة الإسراء











658 ,472

رقم الإيداع لدى دائرة المكتبة الوطنية: (2014/1/542)

المؤلف: محمد عبد حسين الطائي - ينال محمود الكيلاني

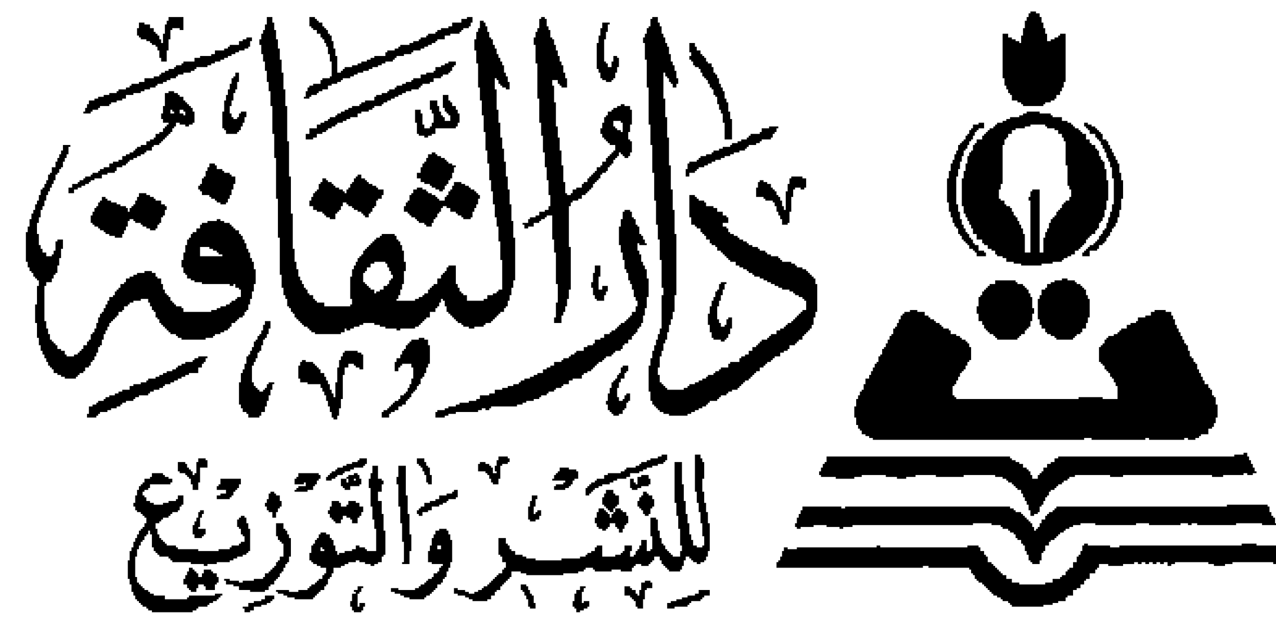
الكتاب: إدارة أمـــن المعلـومـــات

الواصفــات: إدارة المعلومـــات - الأمـــن - القانـــون

لا يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أو الناشر

ISBN:978-9957-16-861-2

الطبعة الأولـــى 2015م - 1436هـ



أسسها خالد محمود جابر حيف عام 1984 عمان - الأردن
Est. Khaled M. Jaber Haif 1984 Amman - Jordan

المركز الرئيسي

عمان - وسط البلد - قرب الجامع الحسيني - سوق البتراء - عمارة الحجيري - رقم 3 د

هاتف: 4646361 6 (962 +) فاكس: 4610291 6 (962 +) ص.ب 1532 عمان 11118 الأردن

فرع الجامعة

عمان - شارع الملكة رانيا العبد الله (الجامعة سابقاً) - مقابل بوابة العلوم - مجمع عربيات التجاري - رقم 261

هاتف: 5341929 6 (962 +) فاكس: 5344929 6 (962 +) ص.ب 20412 عمان 11118 الأردن

Website: www.daralthaqafa.com e-mail: info@daralthaqafa.com

Main Center

Amman - Downtown - Near Hussayni Mosque - Petra Market - Hujairi Building - No. 3 d

Tel.: (+962) 6 4646361 - Fax: (+962) 6 4610291 - P.O.Box: 1532 Amman 11118 Jordan

University Branch

Amman - Queen Rania Al-Abdallah str. - Front Science College gate - Arabiyat Complex - No. 261

Tel.: (+962) 6 5341929 - Fax: (+962) 6 5344929 - P.O.Box: 20412 Amman 11118 Jordan

Dar Al-Thaqafa For Publishing & Distributing

الثقافة للتصميم والإخراج

إدارة أمن المعلومات

الأستاذ الدكتور
محمد عبد حسين الطائي
كليـة الاقتصـاد والعلـوم الإداريـة
جامعـة الزرقـاء

الدكتور
ينـال محمـود الكيـلاني
كليـة العلـوم الإداريـة والماليـة
جامعـة الإسـراء

دار الثقافة
للنشر والتوزيع
1436هـ-2015م

الفهرس

الفصل الأول

أمن المعلومات.. وجهة نظر تاريخية

الفصل الثاني

أمن المعلومات في المؤسسة

الفصل الثالث

حاكمية أمن المعلومات

الفصل الرابع

التهديدات لأمن المعلومات

الفصل الخامس

الأسباب الأخرى لانعدام أمن المعلومات

الفصل السادس

قياس أمن المعلومات

الفصل السابع

موضوعات أمن المعلومات الأخرى

الفصل الثامن

آلية تعزيز أمن المعلومات

المقدمة

واجهت المنظمات في السنوات الأخيرة تحدياً كبيراً تمثل في الانتقال من شبكات المعلومات وهياكل النظم ذات الملكية الخاصة إلى شبكات المعلومات المفتوحة وهياكل النظم ذات الخدمات والزبائن المتنوعة والمتعددة. وعلى الرغم من أن هذه الشبكات زادت من كفاءة هذه المنظمات وعززت موقفها التنافسي في السوق إلا أنها بذات الوقت ـ وبسبب طبيعة البيئات المفتوحة التي تتسم بها ـ زادت من مخاطر أمن المعلومات، إذ يؤكد المتخصصون في مجال نظم المعلومات على حقيقة جوهرية هي أن هذه الشبكات تعد سلاحا ذو حدين، فمن جهة أسهمت في إحداث تغييرات جوهرية متسارعة في أساليب وإجراءات العمل في المنظمات المختلفة عندما أصبحت عملية جمع البيانات من مصادرها المختلفة ومعالجتها وخزن المعلومات وتحديثها واسترجاعها وإيصالها إلى المستفيدين من خلال نظم المعلومات وشبكات الاتصالات المتطورة إحدى أهم السمات في عصرنا الحاضر"عصر ثورة المعلومات". ومن جهة أخرى سهلت هذه النظم والشبكات مهمة اختراق أمن المعلومات وسرقتها أو تحريفها وتشويهها أو إساءة استخدامها أو تسريبها خارج القنوات المخصصة لها أو المرخصة بتداولها والاستفادة منها (Jones,1993:2)، ذلك لأنه لا قيمة لهذه النظم وتلك الشبكات إلا إذا حصلت المشاركة بين المنظمة والمنظمات الأخرى، وبناء عليه فالمنظمات ليست مطالبة بجعل معلوماتها متاحة خارج حدود نظمها وشبكاتها الخاصة فحسب وإنما السماح للآخرين بمراجعة أو تحديث

معلوماتها في شبكاتها الداخلية، أيضا الأمر الذي أتاح الفرصة لإسقاط حواجز الأمن المادية والإلكترونية المعتمدة من قبل المنظمات لحماية أمن معلوماتها، بتعبير آخر، أنه في الوقت الذي تتزايد فيه فرص توظيف المعلومات والاتصالات، فإن التحديات الأمنية تتزايد كذلك. في عام (2007)، تم الإبلاغ عن أكثر من (150000) هجمة على أجهزة الحاسبات المتصلة بالإنترنت لفريق الاستجابة لطوارئ الحاسب المعروف (computer Emergency Response Team) إختصاراً (CERT).ويتوقع هذا الفريق الذي تموله الحكومة ان يتضاعف عدد هذه الهجمات بحلول عام (2009). وفي السوق العالمية فإن الهجوم على جهاز حاسوب واحد لديه القدرة على التأثير في عمليات العديد من النظم المترابطة. في أعقاب (11) سبتمبر من عام (2001)، أصبحت الولايات المتحدة الأمريكية وغيرها من الدول أكثر قلقا بشأن التهديد المحتمل للبنية التحتية الحاسوبية ونظم المعلومات من خلال احتمال إساءة استخدام شبكات الحاسوب والانترنت.

مما سبق وعلى الرغم من أن الرقابة القوية وفرت ضمانات جوهرية لحماية أمن المعلومات والحد من الوصول غير المرخص لها وكذلك التحريف والسرقة إلا أن التطورات الحديثة التي حصلت في نظم المعلومات وشبكات الاتصالات والتي تم تأشيرها في أعلاه قللت من فاعلية الرقابة التقليدية، إذ وجدت هذه المنظمات أن سياساتها الأمنية المطبقة حاضرا بحاجة إلى التطوير أو أنها لم تعد ملائمة لمجاراة تلك التطورات بعد أن أصبحت سياساتها بخصوص أمن المعلومات لا تتناسب مع متطلبات نظمها وشبكاتها المتطورة بكفاءة وفاعلية.

هذا الكتاب موجه لأولئك الذين يسعون إلى الحصول على فهم أوسع لمفهوم أمن المعلومات وما يجب القيام به لحماية أصول/ موجودات المعلومات والدور الذي يجب ان يقوم به. وتهدف هذه الفصول القصيرة إلى إعطاء لمحة موجزة عن مشكلة أمن المعلومات ولماذا لم تحل هذه المشكلة جذرياً، وما يترتب عليها من حيث استخدام أنظمة الحاسب والشبكات في عالم متصل يوجد فيه أكثر من (2) مليار شخص يستخدمون الإنترنت وأكثر من (4) مليارات يمتلكون هواتف نقالة. كثير منهم لديهم أيضا المعرفة الكافية عن طريقة عمل هذه الاجهزةولديهم القدرة على تعطيلها. ولتكريس هذا التوجه تضمن الكتاب ثمانية فصول، تناول الفصل الأول. أمن المعلومات من وجهة نظر تاريخية من خلال بيان الوجود المطلق لتكنولوجيا المعلومات والاتصالات وتبعياته، دلالات أمن المعلومات، والاجابة عن ماذا يحصل في الفضاء الالكتروني، وتوضيح عدم التماثل وعواقبه، إلى جانب تقديم الدروس المستنبطة في السنوات العشر الماضية. وتطرق الفصل الثاني إلى مفهوم أمن المعلومات في المؤسسة، وبيان أبعاد مفهوم أمن المعلومات والمجالات الرئيسة المستهدفة في إنعدام أمن المعلومات، والفرق بين الأمن المادي وأمن المعلومات وأمن تكنولوجيا المعلومات والاتصالات، أهمية إدارة أمن المعلومات، وغايات إدارة أمن المعلومات. واستعرض الفصل الثالث حاكمية أمن المعلومات من خلال تحديد الغرض من حاكمية أمن المعلومات وبيان مكوناتها، مبادئها ومن ثم توضيح أهم قواعد السلوك / معايير أمن المعلومات. واشتمل الفصل الرابع التهديدات لأمن المعلومات، من خلال تعريف التهديدات، وبيان أنواع التهديدات، وتوفير الاجابة عن السؤال من الذي يسرق المعلومات وما هي

المعلومات المستهدفة، إلى جانب توضيح مجالات اختراق أمن المعلومات وتحديد نقاط الضعف في أمن المعلومات. وإستعرض الفصل الخامس الاسباب الاخرى الداخلية و الخارجية لانعدام أمن المعلومات. وتطرق الفصل السادس إلى كيفية قياس أمن المعلومات وإعداد تقارير قياس أمن المعلومات. وتناول الفصل السابع الموضوعات الأخرى لأمن المعلومات مثل تحليل أثر الأعمال، إدارة مخاطر المعلومات، التخطيط من أجل البقاء والمشهد التشريعي. واختتم الكتاب بالفصل الثامن الذي جسد آلية تعزيز أمن المعلومات من خلال سبعة إتجاهات هي على التوالي: صياغة الاستراتيجية الأمنية، التشريع والقانون، الافراد العاملون، إجراءات التعامل مع الملفات الورقية والفاكس، مواجهة الفايروسات، تحديد العمليات الرئيسة وإنشاء وحدات أمن المعلومات.

آملين أن يحقق الكتاب كامل الأهداف المرجوة

المؤلفان

الفصل الأول

أمن المعلومات.. وجهة نظر تاريخية

1

- تمهيد
- أولاً: الوجود المطلق لتكنولوجيا المعلومات والاتصالات وتبعياته
- ثانياً: دلالات أمن المعلومات
- ثالثاً: ماذا يحصل في "الفضاء الإلكتروني"؟
- رابعاً: عدم التماثل وعواقبه
- خامساً: الدروس المستنبطة في السنوات العشر الماضية

الفصل الأول

أمن المعلومات.. وجهة نظر تاريخية

Information security.. Hestorical review

تمهيد:

في هذا الفصل سوف نتطرق إلى التاريخ القصير لتكنولوجيا المعلومات، والعواقب غير المقصودة والآثار الجانبية التي سببتها. ولماذا أصبح أمن المعلومات وأمن تكنولوجيا المعلومات مهماً. وسنوضح أيضاً الجوانب الفنية التي تجعل الفضاء الإلكتروني غير آمن ومن المستحيل عملياً إصلاحه والتحكم فيه بشكل كلي.

أوضح المحرر والمؤلف (Alexander Klimburg) ان الإطار المشكل حول الأمن المعلوماتي الوطني غير محكم، وذكرت منظمة حلف شمال الأطلسي عام (2013) التاريخ القصير لتكنولوجيات المعلومات وآثارها الجانبية المحتملة على أمن دول المنظمة. أولئك الذين عملوا في مختبرات الأبحاث في الستينات والسبعينات والتي تعد الفترة الرائدة في مجال الابتكار التقني، ينظرون إلى تكنولوجيات اليوم باستغراب، إن لم يكن بنظرة شك. فشل العديد من قادة الصناعة بالمشاركة والإقتناع بأن هذه التقنيات سوف تغير العالم. وفي عام (1943)، تنبأ (Thomas Watson)، الرئيس التنفيذي لشركة (IBM)، أنه "سيكون هناك سوق عالمي لمنتجات تكنولوجيا المعلومات والاتصالات ولربما سيحتوي هذا السوق على خمسة أجهزة حاسبات فقط".

في عام (1977)، قال (Ken Olsen)، رئيس شركة المعدات الرقمية ما يلي: "ليس هناك سبب لأي فرد أن يمتلك جهاز حاسوب في المنزل". هذه الشركة لم تعد موجوده في السوق.

هذه النجاحات التحولية شملت الدوائر المتكاملة الرقمية (الرقائق) والإنترنت في منتصف الستينات، والحواسيب الشخصية، وشبكات الألياف البصرية والاتصالات الهاتفية الخلوية في السبعينات. ثم جاءت واجهات المستخدم الرسومية، مثل (Apple Mac) في عام (1984) ونظام التشغيل (Windows) في عام (1990)، والشبكة العالمية (1991)، و(Google) في (1998). ثم تم إطلاق أول نموذج من (Apple iPhone) في عام (2007) وتبعه النموذج الأول من جهاز (iPad) في عام (2010). هذه الابتكارات لم تتوقف، ومن الظاهر أنها ستستمر وبتسارع. تلك البصيرة تكفي للاعتقاد أن هذه التقنيات سوف تحول العالم، وأولئك الذين هم على استعداد للاستثمار فيها قد يصبحون أغنياء بشكل مثير للدهشة. من ناحية أخرى كانت هناك إخفاقات كثيرة في الأفكار والمنتجات والخدمات التي أظهرت إمكانيات كبيرة لكنها لم تنجح. وكم نتذكر شركات مثل (Wang) الشركة الرائدة في معالجة النصوص وأجهزة الحاسبات المصغرة في أواخر السبعينات أو (Altavista)، محرك البحث الذي أطلق في عام (1995).

هذه الموجة السريعة للابتكارات، التي يسميها البعض تيكنامي (Technami) تيمناً بالتسونامي، جلبت معها الآثار الجانبية والعواقب غير المقصودة مثل انعدام أمن المعلومات، وأصبح مدعاة للقلق. وتشمل هذه الابتكارات الحديثة السيارات التي لا تحتاج إلى سائق، وآلات الجراحة

الروبوتية (والتي لا يزال يسيطر عليها الإنسان، ولكن هذا الوضع قد يتغير)، والأجهزة المرنة التي يمكن ارتداؤها والالكترونيات العسكرية.

يتم توفير منتجات تكنولوجيا المعلومات عادةً كما هي، مع ضمانات محدودة، وفي حالة البرمجيات فإن التراخيص تحمي المزود من أي مسؤولية عن العواقب التي قد يسببها خلل أو فشل في هذه البرمجيات. معظم اتفاقيات الترخيص الخاصة بالمستخدم النهائي (EULA) طويلة ويصعب فهمها من قبل الشخص العادي، ويجب على هذا المستخدم الموافقة على الشروط والأحكام لكي يتمكن من تحميل وتنزيل البرنامج. العديد من التطبيقات المصممة للهواتف الذكية والأجهزة اللوحية ربما لم تتح ضمان الجودة الكافية، وبعضها تم انتاجه لإحداث الأضرار وسميت (البرامج الضارة).

وهذا بخلاف الوضع السائد مثلاً في صناعة المستحضرات الصيدلانية حيث أن الترخيص لبيع المنتج يتطلب اختبارات مكثفة ومن ثم بروتوكولات صارمة. وفي حالة بيعها، فإن المنتج يتضمن نشرة تصف الآثار الجانبية المحتملة وموانع الإستخدام. هذه العملية لا تضمن دائما أن تكون المنتجات آمنة بما فيه الكفاية، وتم سحب بعض المنتجات من السوق. ومع ذلك، فإن هذا الإجراء هو أفضل من الوضع السائد في بيع منتجات تكنولوجيا المعلومات والاتصالات والذي يعتمد مبدأ "لقد اشتريت، والآن نتمى لك حظا سعيدا".

أولاً: الوجود المطلق لتكنولوجيا المعلومات والاتصالات وتبعياته

هل يمكن للمرء أن يتصور بيئة اليوم دون تكنولوجيات المعلومات والاتصالات (ICT) والأجهزة النقالة أو الإنترنت؟ هناك أماكن قليلة يوجد بها عدد قليل من الأفراد المتميزين الذين يستفيدون من الوسائل التقنية والمالية،

والعدد آخذ بالتناقص. الأرقام التي نشرتها الإحصائيات العالمية تشير إلى أن التقديرات لأرقام مستخدمي الإنترنت في منتصف عام 2012 كان أكثر من (2.4) مليار مستخدم (هل لاحظت أن تجار المخدرات وصناع تكنولوجيا المعلومات هم الوحيدون الذين يستخدمون كلمة "مستخدم" بدلاً عن عميل). هنالك مصادر أخرى تعطي أرقام للمقارنة. هناك تقرير صادر عن الاتحاد الدولي للاتصالات، وهي منظمة تابعة للأمم المتحدة، ويذكر هذا التقرير أنه في أكتوبر 2012 كان هناك أكثر من (6) مليار مشترك في الهاتف المحمول. في ذلك الوقت كان عدد سكان العالم يزيد قليلا عن (7) مليارات، وكثير منهم يعيشون بدخل أقل من (2) دولار في اليوم.

لقد أصبح وجود المعلومات والتقنيات التي يسمح بالوصول إليها من العناصر الأساسية، ليس فقط للأفراد ولكن أيضا بالنسبة للدول والشركات من جميع الأنواع. وإن الحماس لوجود الأدوات والخدمات الجديدة يتحدى المعتقد. إطلاق منتج جديد مثلاً يمكن أن يسبب وقوف الزبائن في طوابير ليلة وضحاها في الشارع تنتظر المتجر لكي يفتح ابوابه. في حين أن التكنولوجيات ليست مثالية وهذا قد لا يكون واضحا لعامة الناس. إلى جانب ذلك، فإن الطرق التي يتبعها المستخدمون لحماية أنظمتهم وبياناتهم ليست مثالية كما هو حال الجميع. الكثير من الاشخاص أيضاً غير مدركين لدورهم في حماية معلوماتهم الشخصية ومعلومات الشركة التي يعملون بها.

ثانياً: دلالات أمن المعلومات The semantics of information security

مفردات أمن المعلومات لا تزال في طور النمو. وهناك جزء كبير منه يتكون من المصطلحات الفنية، على سبيل المثال، (botnet, rootkit) الجذور

الخفية، المفتاح العمومي، الخ وهذه المصطلحات هي ذات معنى إلى حد ما بالنسبة لمن ينشئها ولكنها غامضة للاخرين. وقد اعتمدت وسائل الإعلام كلمة "الانترنت" واستخدمتها على نحو متكرر. وقد اعتمد الساسة هذا المصطلح على الرغم من أن هناك أيضا تعريفات متعددة ومتناقضة له إلى حد ما. عندما أوجد (William Gibson) كلمة "الفضاء الإلكتروني (Cyberspace)" عام (1984) في روايته (Neuromancer) فإن هذه الكلمة ساء استخدامها بشكل كبير دون إستفسار عن معناها الصحيح. في وقت لاحق من حياته قال (William Gibson) أنها كانت "كلمة طنانة وبلا معنى أساسا".

لا يوجد تعريف متفق عليه لمصطلح "الفضاء الإلكتروني". وهو يتضمن بالتأكيد عوالم البيانات والبرمجيات. ويرى البعض أنه يتضمن أيضا البنية التحتية لشبكة الاتصالات والحاسبات. وهناك شبه إجماع على أن شبكة الإنترنت هي جزء من الفضاء الإلكتروني وأن الإنترنت ليست سوى عنصر من ذلك. وبالمثل هناك اتفاق محدود حول تعريفات مصطلح " حرب الفضاء cyber-war " و "الإرهاب الفضائي cyber-terrorism " وهنا عدم اتفاق على كيفية تهجئة هذه المصطلحات: هل يتم تهجئتها بوصفها كلمتين (الحرب الفضاء)، على النحو الوارد في أعلاه أو ككلمة واحدة (الحرب الفضائية). مثل هذه الامور مهمة للمشرعين والدبلوماسيين والمحامين.

هناك إجماع محدود على تعريف مصطلح الأمن الفضائي (cyber security) (بغض النظر عن كيفية تهجئته). في هذا الكتاب، سوف تستخدم مفاهيم "أمن المعلومات" و "أمن تكنولوجيا المعلومات" في جميع أجزاء الكتاب ويتم مناقشتها في الفصل الثالث. الغموض والالتباس اللغوي لا ينتهي هنا

طالما أن هناك مصطلحات أخرى تستخدم أيضا بحرية دون تعاريف مقبولة على نطاق واسع ومتفق عليها. مثال على هذه المصطلحات الأخرى هو "القرصان hacker " الذي يمكن أن يكون أي شخص، في أي مكان:

- يمكن أن يكون القرصان مبرمج الحاسب الذي يجمع بين الفضول والمعرفة والإبداع والذكاء لتحقيق هدف معين. كان هذا هو المعنى الأصلي للمصطلح.
- يمكن أيضا أن يكون القرصان شخص يتجاوز أو يتداخل مع أمن الحاسب و/أوالبرمجيات والبيانات.
- مجموعة من المتسللين الشباب مع بعض المعرفة في الحاسوب ويطلق عليهم اسم (Script Kiddies)، وذلك باستخدام الأدوات المتاحة عبر الإنترنت.
- آخرون يعملون كمجموعات يشار إليها (Hacktivists)، (واحدة من هذه المجموعات تطلق على نفسها "المجهولون"؛
- ثم تأتي مرتزقة الفضاء، رجال الأمن المحترفون الذين يعملون مع المجرمين.
- هناك من يعملون في المنظمات العسكرية والقانونية - غالباً ما يشير إليهم وسائل الإعلام بأنهم "جيوش الفضاء".
- هناك أيضا أولئك الذين يعملون للجهات الفاعلة من غير الدول ("الإرهابيين").

ولتعقيد الأمور، يمكن أن يتقمص شخص واحد عدد من الأدوار أعلاه في وقت واحد.

ثالثاً: ما ذا يحصل في "الفضاء الإلكتروني" (Cyberspace)"؟

يعتقد الكثير من الناس أن نظم المعلومات سوف تعمل على نحو سليم كما هو مخطط لكي تعمل عند القيام بتصميمها. فهم يفترضون أن النظام سوف يعمل بشكل موثوق وأن المعلومات التي سوف يوفرها تكون صحيحة. عندما يتم إثبات أن هذه الافتراضات خاطئة ويتعذر تحققها، يمكن أن تكون العواقب كارثية. خاصة إذا ما خذنا بعين الاعتبار العديد من الأمور غير المرغوب فيها والتي تحصل في الفضاء الإلكتروني في وقتنا الحاضر. القائمة التالية ليست شاملة حيث أن براعة الإنسان قادرة على تطوير طرق جديدة لاستغلال انعدام الأمن:

- الخسارة المالية: في عام (1995) أصبح البنك البريطاني صاحب التاريخ الطويل خارج ميدان العمل، ثم في عام (2008) خسر البنك الفرنسي أكثر من (6) مليارات يورو. في عام (2011) خسر البنك السويسري الذي كان يعمل في لندن (2) مليار دولار. الحالات الثلاث حصلت من خلال إساءة الاستخدام الداخلي أو سوء المعاملة. ولم تكن هذه الحالات فريدة من نوعها.
- هجمات الحرمان من الخدمة: وهذه الهجمات تقود إلى إغراق النظام، وعادة ما يكون إما موقع على شبكة الانترنت أو خدمة البريد الإلكتروني بحيث لا يمكن أن يعمل. مثل هذه الهجمات هي من السهل تنفيذها بما فيه الكفاية وعادة ما تكون ناجحة.
- تخريب شبكات أو أنظمة الحاسوب للتدخل في عملها، أو تدمير بيانات أو برمجيات المنظمة إلى جانب استخدام البرمجيات الخبيثة للسيطرة على نظام الحاسوب للعديد من الأسباب المحتملة.

- سرقة الملكية الفكرية: بما في ذلك التجسس الصناعي، و سرقة المعلومات الشخصية، التي تمثل خرقاً للخصوصية، إلى جانب إلحاق الضرر بالجهاز الشخصي بوساطة البرمجيات الخبيثة، فضلاً عن فقدان السيطرة على الجهاز الشخصي الذي يتم استخدامه بدون معرفة وعلم المجني عليه بنشر الرسائل غير المرغوب فيها أو تنفيذ الحرمان من الخدمة (zombie, botnet).
- هناك مخاوف متزايدة بشأن تهديد الهجمات الالكترونية (cyber attacks)على البنية التحتية الحيوية مثل المرافق العامة (الكهرباء، والمياه، والاتصالات، والنقل، والمستشفيات، وغيرها) وكذلك على تنفيذ القانون وخدمات الطوارئ. ويتفق السياسيون في جميع أنحاء العالم أيضا على أن هناك تهديدا لبعض الكيانات التي تلعب دورا حاسما في الأمن القومي، مثل المنشآت العسكرية والعمليات الحربية في الميدان، والتي قد تكون هدفا للهجوم عبر الانترنت. الأفراد هم أيضا يمثلون أهدافا لمثل هذا الهجوم، على سبيل المثال:
- الانتحال: تم إنشاء صفحات (Face book) لكبار المسؤولين التنفيذيين في الإنتربول، ومنظمة حلف شمال الأطلسي ـ من دون علمهم أو موافقتهم ـ واستغلالها للحصول على "الأصدقاء". وقد تم إستخدامها بعد ذلك لتوفير المعلومات. كان الأفراد المعنيين لا يدركون هذا. إساءة استخدام الثقة – قام باحث أكاديمي بإنشاء حسابات على صفحات (Facebook)، التغريد (Twitter)، لينكدإن (Linkedin) ووسائل الاعلام الاجتماعية الأخرى لامرأة

شابة مع صفات مثيرة للإعجاب. قام العديد من المشتركين بمحاولة التواصل معها وبعضهم قام بعرض وظيفة عليها أو إرسال وثائق حساسة لطلب رأيها. في الواقع روبين لم تكن موجودة وكانت هويتها جزء من البحث في كيفية استخدام الثقة وسوء المعاملة في الشبكات الاجتماعية.

- الابتزاز: على سبيل المثال من خلال تشفير البيانات في الحاسبة والمطالبة بالدفع لتوفير مفتاح فك التشفير، أو سرقة الهوية، بما في ذلك بيانات عن الحسابات المصرفية، وبطاقات الائتمان، وما إلى ذلك، إلى جانب الهجمات على الهواتف المحمولة والهدف الأساسي هو السرقة المالية. إلخ

رابعاً: عدم التماثل وعواقبه Asymmetries and consequences

تنطوي حالة عدم التماثل على العديد من المزايا، كما أن لها تبعات (عواقب) معينة. فالمزايا بالنسبة للمهاجم يمكن أن تكون:

1- عدم وجود الحاجة لتواجد المهاجم وحضوره بدنياً (شخصياً) في الموقع لتنفيذ الهجوم، بالطبع مع مراعاة بعض الاستثناءات (على سبيل المثال عندما لا يكون الهدف مرتبطاً بشبكة عالمية مثل شبكة الإنترنت)، كان هذا هو الحال في المفاعل النووي لموقع "نطنز" في إيران، حيث تم عزل أنظمة التحكم في أجهزة الطرد المركزي للتخصيب من الإنترنت، وعندها تم إدخال البرامج الضارة باستخدام جهاز ذاكرة فلاش.

2- عدم وجود عقوبة للفشل: كل تفاعل مع دفاعات شبكة الحاسب أو النظام يوفر للمهاجم الأفكار التي تساعده في إعداد هجمات لاحقة.

3- عدم وجود معوقات إدارية للتغلب على المهاجم: فالمورد الرئيسي للمهاجمين هو المعرفة وأن متطلباتهم من الأدوات والتكنولوجيا متواضعة، كما أن مهمة اقتنائها والحصول عليها من المؤكد أن تكون أبسط من عقود مشتريات الشركات، التي تستلزم مستويات مختلفة من الموافقات الادارية. اؤلئك المسؤولين عن الحفاظ على أمن أصول/موجودات المعلومات غالبا ما يواجهون معوقات بسبب عوامل أخرى، أبرزها:

- الضغط لاحتواء التكاليف أو خفضها.
- عدم القدرة على تطوير حالات تجارية قوية لتبريرالنفقات والحصول على الموارد

خامساً: الدروس المستنبطة في السنوات العشر الماضية

Lessons identified in the last ten years

من خلال الاستعراض التاريخي لجهود إدارة أمن المعلومات سواء على مستوى الكتابات أو على مستوى التطبيقات يمكن استخلاص العديد من الدروس، وأهمها نوجزها في الاتي:

- "الفضاء الإلكتروني" والذي يتصف بأنه غير آمن بطبيعته، يعد مصطلحاً غامضاً ويمكن أن يؤدي إلى سوء الفهم والارتباك. فالعديد من المصطلحات الأساسية يمكن أن نجد لها تعريفات

مختلفة (على سبيل المثال حرب الفضاء وسلاح الفضاء). نفس الشيء ينطبق على مفهومي "أمن المعلومات" و "أمن تكنولوجيا المعلومات".

- أصبح الاعتماد على نظم المعلومات والخدمات والتكنولوجيا لا رجعة فيه. وهناك معرفة كافية حول كيفية حماية هذه الأنظمة والخدمات من خلال العديد من المعايير والممارسات الجيدة والمبادئ التوجيهية. ومع ذلك، فإن هناك الحاجة إلى الكثير مما ينبغي القيام به لتطبيق هذه المعرفة في الممارسة العملية.
- هنالك أطراف عديدة ترغب في تعطيل نظم المعلومات والاضرار بمحتوياتها من المعلومات، ويمكن أن تكون هذه الاطراف أي شخص وفي أي مكان، وإنه من الحكمة أن نفترض أنهم موهوبون، ولديهم المعرفة، الدوافع والحرص والمثابرة للوصول إلى أهدافهم، وربما أكثر من حرص وتفاني الأشخاص المسؤولين عن الحفاظ على الأمن في المنظمة.
- المتخصصون في مجال الأمن والإدارة العليا لديهم تصورات مختلفة تتعلق بأهمية هذا الموضوع. وبسبب ضعف الحوار وأيضا ضعف حاكمية أمن المعلومات، فإن العديد من المنظمات غير مستعدة بشكل جيد للرد على أي حادث أمني قد تواجهه.
- لا يمكن تحقيق أمن للمعلومات بنسبة مطلقة (100٪)، ولكي نستطيع الوصول إلى درجة عالية من أمن المعلومات فإننا نحتاج إلى

أربعة مكونات أساسية، هذه المكونات هي: الحاكمية، الافراد، العمليات والتكنولوجيا.

- أصبحت ممارسة أمن المعلومات مهنة مستقرة ومعترف بها ولكن لم يتم وضع أنظمة وقوانين تقوم بتنظيمها. خلافا للطبيب في الطب أو الطيار الذي يحلق بالطائرات، فيمكن لأي شخص أن يكون ممارس لهذه المهنة.
- سرعة الابتكار التقني والحماس للمنتجات الجديدة يتم تسخيرها للتآمر ضد "الأمن عن طريق التصميم"، والذي يعد بدوره غائباً إلى حد كبير في المنتجات التي تعتمد على الفضاء الإلكتروني. ففي الصناعات الآمنة، يتم التحقيق في الحوادث التي تحصل بدقة وذلك لإكتشاف السبب الأساسي لهذه المشكلة، والتي يتم معالجتها بعد ذلك بالتعديل على التصميم.
- يجب فهم وقياس أثر الأحداث الأمنية على المنظمة (ويشار هنا إلى تحليل الأثر على الأعمال) وأهميتها الجوهرية وذلك لضمان أن التدابير الوقائية وإجراءات الحماية يتم تطبيقها حسب الحاجة.
- أمن المعلومات يتعامل مع حالة عدم التأكد بدلا من حالة المخاطرة، كما يتم استهداف الحوادث المحتملة التي يتوقع حدوثها، عليه فان المشكلة هنا تكمن في ضعف وعجزالقدرة البشرية لتقديم تنبؤات مستقبلية لهذه الحوادث المحتملة، حيث أن الشركات لديها سجل ضعيف في هذا المجال كما اشارت إلى ذلك نتائج العديد من الدراسات الميدانية.

- أمـن المعلومـات لـيس مهمـة شـخص معـين، بـل هـي مهمـة الجميـع، فالجميع لديه دورمعين بغض النظر عن طبيعة هذا الدور وحجمه ودرجة تأثيره. والكثير من الاشخاص قد لا يعون هذه الحقيقة.

أسئلة الفصل

س (1): أذكر بعضاً من نماذج النجاح وحالات الاخفاق في منتجات تكنولوجيا المعلومات والاتصالات.

س (2): يتم توفير منتجات تكنولوجيا المعلومات والاتصالات في العادة وبخلاف (مثلاً المنتجات الصيدلانية) مع ضمانات محدودة، علق على العبارة معززاً اجابتك بالامثلة.

س (3): كيف تبرهن على خاصية الوجود المطلق لمنتجات تكنولوجيا المعلومات والاتصالات.

س (4): ما هي من وجهة نظرك أهم التبعات المترتبة على الوجود المطلق لمنتجات تكنولوجيا المعلومات والاتصالات؟

س (5): يشير المتخصصون في أمن المعلومات إلى أن مفردات أمن المعلومات لا تزال في طور النمو، كيف؟

س (6): هل هناك تعريف متفق عليه لمصطلح (الفضاء الالكتروني)، ولماذا؟

س (7): من هو القرصان (Hacker) في بيئة أمن المعلومات؟

س (8): هل تعتقد أن نظم المعلومات بعد إستخدامها سوف تعمل بشكل موثوق؟

س (9): وضح باختصار أهم المزايا التي تتيحها خاصية عدم التماثل في بيئة أمن المعلومات لمن يرغب باختراق أمن المعلومات.

س (10): أجب بوضع إشارة (صح) أو إشارة (خطأ) أمام العبارات الآتية:

	العبارات	الاشارة
1	"الفضاء الإلكتروني" والذي يتصف بأنه غير آمن بطبيعته، يعد مصطلحاً غامضاً	
2	مفهومي "أمن المعلومات" و "أمن تكنولوجيا المعلومات". يعدان من المفاهيم الواضحة	
3	أصبح الاعتماد على نظم المعلومات والخدمات والتكنولوجيا موضع شك يجب إعادة النظر فيه من جديد	
4	هناك الحاجة إلى الكثير مما ينبغي القيام به لتطبيق المعرفة الخاصة بأمن المعلومات في الممارسة العملية.	
5	من الحكمة أن نفترض أن الذين يسعون إلى إختراق أمن المعلومات موهوبون، ولديهم المعرفة والدافع لتحقيق ذلك	
6	يمكن تحقيق أمن للمعلومات بنسبة مطلقة(100٪)،	
7	يمكن الوصول إلى درجة عالية من أمن المعلومات من خلال تحقيق الحاكمية فقط	

8	أصبحت ممارسة أمن المعلومات مهنة مستقرة ومعترف بها ولها أنظمة وقوانين تقوم بتنظيمها. كما هو الحال بالنسبة للطبيب أو الطيار	
9	المنتجات التي تعتمد على الفضاء الإلكتروني تعد ضمن فئة الصناعات الآمنة	
10	أمن المعلومات يتعامل مع حالة عدم التأكد بدلا من حالة المخاطرة	
11	تشير نتائج الدراسات إلى أنه يمكن تقديم تنبؤات دقيقة بالحوادث المحتلمة لأمن المعلومات	
12	يعد فهم وقياس أثر الأحداث الأمنية على المنظمة مهماً للغاية لضمان أمن المعلومات	
13	أمن المعلومات في المنظمة وظيفة الجميع وليس فقط وظيفة ضابط أمن المعلومات	

الفصل الثاني

أمن المعلومات في المؤسسة

2

- تمهيد
- أولاً: المقصود بـ" أمن المعلومات"
- ثانياً: أبعاد مفهوم أمن المعلومات
- ثالثاً: المجالات الرئيسة المستهدفة في انعدام أمن المعلومات
- رابعاً: الفرق بين الأمن المادي وأمن المعلومات في المؤسسة وأمن تكنولوجيا المعلومات والاتصالات
- خامساً: غايات إدارة أمن المعلومات

الفصل الثاني

أمن المعلومات في المؤسسة

information security in the enterprise

تمهيد:

يعمل المجتمع على أساس من الثقة، وهو موضوع معقد مع الآثار الأخلاقية والاجتماعية المقترنة بها. والثقة تمثل الاعتقاد في الصدق والنزاهة وحسن النية من قبل الأطراف المعنية. حيث تبين لنا في الفصل الأول أن الثقة في الفضاء الإلكتروني قد تم تجاهلها متعمداً في كثير من الأحيان على مدى سنوات عديدة. وقد أدى فقدان الثقة إلى تطوير المعايير والممارسات الجيدة والمبادئ التوجيهية وسياسات أمن المعلومات، والتشريعات وغيرها من التدابير التي تعد ضرورية لحماية أصول/ موجودات المعلومات.

(الثقة بالآخرين جيدة. لكن عدم الثقة أفضل) مثل إيطالي

يقدم هذا الفصل إرشادات حول مفهوم أمن المعلومات والأبعاد الجوهرية لهذا المفهوم، والمجالات الرئيسة لانعدام أمن المعلومات والاختلاف بين مفاهيم أمن المؤسسة وأمن المعلومات وأمن تكنولوجيا المعلومات والاتصالات، والجوانب التي يمكن من خلالها تجسيد أهمية إدارة أمن المعلومات والغايات الرئيسة لأمن المعلومات.

أولاً : المقصود بـ "أمن المعلومات"

What is meant by “Information Security

في الفصل السابق تمت مناقشة "الأمن" دون التطرق إلى تعريف هذا المفهوم، على افتراض أن مثل هذا المفهوم هو مفهوم شائع وأن الجميع يدرك ما يعنيه. ولكن للأسف، هذا ليس صحيحا تماما بسبب الغموض اللغوي والارتباك الذي ينطوي عليه هذا المفهوم، إذ يشير (Parker, 1997) إلى أننا بوصفنا متخصصين في أمن المعلومات فأنه يجب علينا تقديم تعريف ووصف عام لمصطلح "أمن المعلومات" لإداراتنا وزبائننا وصحفيينا ونظرائنا في الحقول الأخرى بل لعائلتنا أيضا. عليه أورد هذا الباحث تعريفات متعددة الأغراض بحيث يتناسب كل تعريف مع ما يعنيه بالنسبة لكل جهة ذات علاقة، وفيما يأتي نعرض هذه التعاريف:

- هي المحافظة على اتاحة المعلومات وسلامتها وسريتها وملكيتها والاستفادة منها.
- هي المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو إلغاؤها أو سوء استخدامها أو الفشل في استخدامها أو الوصول إليها أو إظهارها أو مراقبتها أو نسخها أو سرقتها.
- هي معالجة جميع الخروقات المذكورة في التعريف الثاني أعلاه قانونيا بشكل ناجح من قبل مالك هذه المعلومات بوصف هذه الخروقات انتهاكا لحقوق المالك.

- هي الوظائف التي تهدف إلى حماية المعلومات والتي تشتمل على التجنب، المنع، الكشف، الإعاقة، النقل، التحويل، الاسترجاع، التصحيح، والإقرار.
- هي الإجراءات التي تحقق الحماية والتي يجب توجيهها من خلال الوفاء بالمعايير المحددة في إطار التشخيص السليم للسلبيات والتهديدات.
- هي الحماية الدقيقة والتي غالبا ما تنجز من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة الأمنية وتطبيقها بفاعلية في إطار استخدام مجموعة من القواعد الرقابية كإرشادات توجه جهود الحماية.

وبنفس الاتجاه يصنف خبراء آخرون تعريفات أمن المعلومات في العديد من المجموعات على النحو التالي:

1- تعريف مجلة (CPA journal) لأمن المعلومات :

عرّفت هذه المجلة أمن المعلومات في خمسة أجزاء هي :

- تعني الحفاظ على توافرالمعلومات وفائدتها ونزاهتها وأصالتها، وسريتها وحيازتها.
- تعني حماية المعلومات من الدمار والتداخل في الاستخدام، واستخدام بيانات غير صحيحة، تعديل واستبدال وتحريف المعلومات وسوء الاستخدام والفشل في الاستخدام، والوصول اليها، الإفشاء والمراقبة والنسخ والسرقة وتعريضها للخطر. الأمن قد يكون أيضا ضمان أن أياً من هذه الانشطة المذكورة أعلاه تنجز بنجاح وقانونيا إذا رغب المالك الشرعي للمعلومات بذلك.

- الوظائف لتحقيق الحماية وهي التجنب والردع والوقاية والكشف والتخفيف والتحويل والمعاقبة عليه، والتصحيح.
- الجهود الرامية إلى تحقيق الحماية والتي يتم الاسترشاد بها من خلال تلبية معيار العناية الواجبة وتحديد نقاط الضعف والتهديدات المادية.
- الحماية الحكيمة يتم إنجازها في الغالب عن طريق إيجاد الضوابط الأمنية والممارسات المعروفة وتطبيقها بشكل فاعل، و باستخدام مجموعة من مبادئ الرقابة كمرشدات.

2- مسرد أمن نظم المعلومات الوطنية في الولايات المتحدة الأمريكية:

U.S.A. National Information Systems Security Glossary

إدارة أمن المعلومات هي: حماية نظم المعلومات من الوصول غير المصرح به لتعديل المعلومات، سواء في التخزين وعملية المعالجة أو نقلها، وضد الحرمان من الخدمة للمستخدمين المرخص لهم أو توفير الخدمة للمستخدمين غير المصرح به، بما في ذلك تلك التدابير اللازمة للكشف عنها، توثيقها، ومواجهة مثل هذه التهديدات.

3- التعريف القانوني Legal definition:

يغطي مفهوم إدارة أمن المعلومات من وجهة النظر القانونية الالتزامات باتخاذ التدابير الملائمة لغرض الحفاظ على وضع الامور مقابل المستوى المطلوب من الأمن، و خاصة، حماية الحقوق المتصلة بالأصول/ الموجودات المعلوماتية. وتتكون هذه الأصول من البيانات الخام التي نظمت في صيغة وثائق، والوسائط و الحقوق المتعلقة باستخدام المحتويات الفعلية.

4- تعريف التقنية العامة General Technical Definition:

أمن المعلومات هو حالة من الأوضاع التي تكون فيها المعلومات، وتجهيز المعلومات والاتصالات لكي تكون محمية في إطار السرية والتمامية وتوافر المعلومات ومعالجتها ضمن سياق شبكات المعلومات. هذا يشمل أيضا تحديد هوية وأحقية الفرد وعدم تغيير البيانات. أمن المعلومات له عدة أبعاد ومستويات. الأبعاد أو المكونات المختلفة تشمل جملة أمور هي: أمن الأجهزة، أمن البرمجيات، الأمن الإداري، الأمن المادي، أمن التشغيل، أمن الأفراد، أمن الاتصالات، وأمن موارد البيانات.

5- تعريف أمن المعلومات:

بناء على ذلك، ولغرض هذا الكتاب نعرف أمن المعلومات على النحو التالي:

" الجهود الرامية إلى حماية موارد معلومات المنظمة من سوء الاستخدام من قبل الأطراف غير المصرح لهم من خلال تحديد التهديدات التي قد تواجه أمن المعلومات وتشخيص نقاط الضعف التي يعاني منها برنامج أمن المعلومات ومن ثم تحديد المخاطر المترتبة على تلك التهديدات واستغلال نقاط الضعف، ووضع سياسة أمن المعلومات وتنفيذ الضوابط والمعاييرالتي تسهم في تعزيز أمن المعلومات.

ثانياً: أبعاد مفهوم إدارة أمن المعلومات

اعتمادا على التعريفات المذكورة في أعلاه يمكننا تحديد الأبعاد الرئيسية لمفهوم أمن المعلومات على النحو الآتي:

1- يميل معظم تعاريف أمن المعلومات إلى التركيز ـ على وجه الحصر في بعض الأحيان ـ على إستخدام محدد، أو وسائل معينة؛ على سبيل المثال، " حماية البيانات الالكترونية من الاستخدام غير المصرح به ". في واقع الأمر هذا الاعتقاد خاطئ، أو ينم عن سوء الفهم، ذلك لأن أمن المعلومات هو مرادف لأمن الحاسوب في أي من مظاهرها: الحاسوب و أمن الشبكات، وامن تكنولوجيا المعلومات (IT)، أمن نظام المعلومات، أمن تكنولوجيا المعلومات والاتصالات (ICT). لكل من هذه المظاهر تركيز مختلف في تجسيد مفهوم أمن المعلومات، ولكن الاهتمام المشترك هو أمن المعلومات في شكل ما (والشكل المقصود هنا هو" الإلكترونية " في كل هذه الحالات) وبالتالي، فإنها كلها تمثل مفاهيم فرعية من مفهوم أمن المعلومات. وعلى العكس، يغطي أمن المعلومات ليس فقط المعلومات ولكن كل البنى التحتية التي تسهل استخدامها، والعمليات، والنظام، والخدمات، والتكنولوجيا وغيرها، بما في ذلك شبكات الحواسيب، والصوت والبيانات، الخ.

2- يهتم أمن المعلومات بتحقيق أمن كافة موارد المعلومات في المنظمة (الحاسوبية والمعدات غير الحاسوبية، والبيانات والمعلومات) من خلال الجهود المبذولة لتحقيق مجموعة من الغايات الجوهرية هي السرية، التوافر، السلامة، المسؤولية وقابلية التدقيق. و تشمل جهود إدارة أمن المعلومات الحماية اليومية، والتحضير للتشغيل بعد حصول الحدث لضمان استمرارية العمل في إطار استراتيجية

مكونة من أربعة خطوات متكاملة هي تحديد المخاطر، تحديد التهديدات المترتبة على هذه المخاطر، وضع سياسة أمن المعلومات وتنفيذ الضوابط والمعايير التي تسهم في تعزيز أمن المعلومات.

3- النقطة المهمة هنا أن أمن المعلومات هو بطبيعته و بالضرورة، ليس بالمحكم ولا بالمانع الذي لا لبس فيه ولم يبلغ حد الكمال. فلا أحد يستطيع القضاء على خطر الاستخدام غير السليم أو الاستخدام المتقلب للمعلومات. إذ ينبغي أن يكون مستوى أمن المعلومات المطلوبة في أي حالة معينة يتناسب مع قيمة المعلومات ومع فقدانها أو القيمة المالية أو خلاف ذلك، والتي يمكن أن تتحقق من الاستخدام غير السليم أوالكشف عنها، تشويهها، حجبها، أو غير ذلك. وفي الواقع أنه من غير الممكن أن يكون هناك نظام أمن مثالي تماما، وبالتالي يتطلب الأمر الحد من الضرر في حالة حدوث أي ضرر يترتب على وجود الخرق لأمن المعلومات.

4- تشير عملية صياغة الضوابط إلى ضرورة وجود الاستراتيجية الملائمة لأمن المعلومات في المنظمة، ويجب ان تتناسب هذه الاستراتيجية مع طبيعة تكنولوجيا المعلومات ومع طبيعة تطبيقاتها في نظم المعلومات وفي شبكات الاتصالات المستخدمة في المنظمة، كما يفترض تعديل هذه الاستراتيجية بما يتلاءم والتغييرات الحاصلة في هذه التكنولوجيا وفي تطبيقاتها.ويؤكد هنا (Palmer, 2001:15) على وجود الحاجة الماسة إلى إطار استراتيجي عملي وشامل لأمن المعلومات يتصف بهيكلية وصياغة جيدتين وسهلة الفهم والإدراك من قبل أعضاء المنظمة.

5- تحديد الجهة المسؤولة عن هذه الصياغة مع ضمان مشاركة جميع الأطراف ذات العلاقة ، ويرى (Parker, 1997:17) أن الذين يسهمون في صياغة هذه الاستراتيجية ويتحملون مسئوليتها هم المالكون لها والمؤتمنين (القائمين عليها) والجهات التي تقدم الخدمات والمستفيدين منها إلى جانب الجهات المساندة الأخرى وهم المختصين في أمن المعلومات والمدققين ومنفذي القوانين وغيرهم من المساعدين. و لاجل تفعيل هذه المشاركة فان الضرورة تقتضي جعل مسألة أمن المعلومات جزءا أساسا من الوصف الوظيفي في المنظمة وان تكون عاملا حاسما في الأداء والتقييم الوظيفي وفي الترفيع ومنح المكافئات، وبخلافه فانه قد ينظر إلى هذه المسألة على أنها غير ضرورية أو معوقة للإنتاج وستطبق كمسألة جمالية فقط وليست ضرورية.

6- تتعدد الجهات التي تخترق أمن المعلومات إلى الحد الذي قد يتعذر معه أحيانا الكشف عن الجهة الحقيقية التي تقف وراء هذا الاختراق، ويشير إلى هذه الحقيقة الباحث (Hill, 1995: 15) بقوله أن هؤلاء الذين لم يعتادوا على حجم المشكلات الملازمة لامن المعلومات قد لا يمتلكون فكرة واضحة عن تلك الجهات التي تخترق أمن المعلومات، وهذه الجهات يمكن تعدادها على النحو الآتي: الأفراد العاملون في مهام الاستلام والتسليم، المحققون، الزائرون بهدف الإطلاع، المستشارون، عملاء وجواسيس المنافسين، الأفراد العاملون (المبرمجون، موظفوا البريد ، موظفوا أمن

المعلومات، البوابون)، زوجات الأفراد العاملين وأقربائهم، الأفراد الساخطون الذين انتهت علاقتهم بالمنظمة وخرجوا من العمل.

7- تتباين الجوانب التي تثير الاهتمام لاختراق أمن المعلومات بتباين طبيعة المعلومات التي تكون عرضة للاختراق، ففي المستشفيات ينصب الاهتمام على سجلات المرضى، وفي مجال التسويق تكون استراتيجيات التسويق هي المهمة، وتستحوذ الأسرار الصناعية في العمليات الصناعية والإنتاجية على الاهتمام الأكبر. ويرى (Hill, 1995: 15-16) أن أهم الموارد المنظماتية التي تثير الاهتمام لسرقة المعلومات هي: قوائم الزبائن، المعلومات المستنسخة، مراسلات المدير التنفيذي، بيانات البحث والتطوير، مشاريع الموازنة، البيانات المالية، الصفقات القانونية، سجلات الأفراد والخطط التسويقية.

8- كما تتعدد أنواع الخروقات لأمن المعلومات (كما سنأتي إلى تفاصيلها في الفصل الرابع) تبعا لخمسة أسس جوهرية هي: طرق اختراق أمن المعلومات، مجالات اختراق أمن المعلومات، طبيعة عرض المعلومات، الطرق المستخدمة في معالجتها، تحديثها، استرجاعها، توصيلها إلى المستفيدين، استخدامها، والرقابة عليها ومصادر هذه المعلومات.

9- لم يظهر أمن المعلومات بحالته الراهنة منذ بداية ظهور الحاسوب لكنه تدرج في إهتمامه ونطاقه، ويمكن إختصار هذا التدرج في أربعة مراحل كما هو موضح في الجدول الآتي:

المرحلة	طبيعة التركيز	طبيعة الاهتمام
الاولى	أمن تشغيل الأجهزة	الأمن يدور حول تحديد الوصول، أو الإطلاع على المعلومات، وذلك من خلال منع الأشخاص الخارجيين من التلاعب أو الإعتداء على الأجهزة، وتوفير البيئة الملائمة والمناخ المناسب.
الثانية	أمن الحاسوب ذاته	الإجراءات المختلفة لضمان أمن مواقع الحواسيب ومرافقها وتسهيلاتها.
الثالثة	أمن البيانات	تركيز الأمن بعد التوسع في إستخدامات الحاسوب وتطبيقاته على البيانات وحمايتها.
الرابعة	أمن المعلومات	المحافظة على المعلومات، سريتها، تماميتها واتاحتها.

الجدول (2 ـ 1)

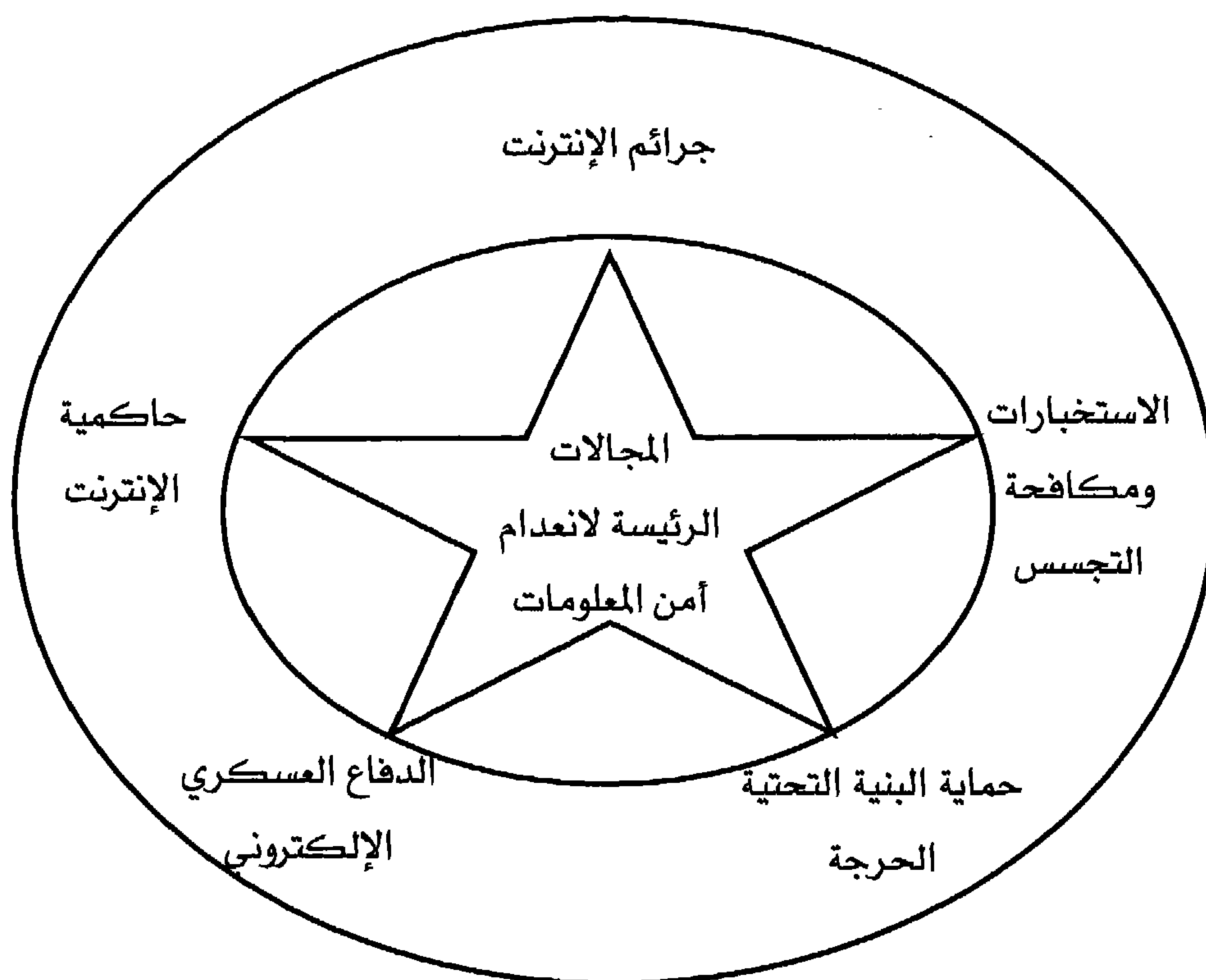
مراحل تطور مفهوم أمن المعلومات ومجال إهتمامه

ثالثاً: المجالات الرئيسة المستهدفة في انعدام أمن المعلومات

The major target areas in information Security

هناك خمسة مجالات رئيسة لانعدام أمن المعلومات سيتم مناقشة كل منها على حدة نظراً لكون المتطلبات والإجراءات مختلفة، وهذه المجالات هي: جرائم الإنترنت، حماية البنية التحتية الحرجة، الدفاع العسكري الإلكتروني، الاستخبارات ومكافحة التجسس، وحاكمية الإنترنت. وفي

هـذا الكتاب سيتم التطرق إلى المجالات الثلاثة الأولى فقط نظرا لمحدودية توافر المعلومات العامة عن الاستخبارات ومكافحة التجسس، والطبيعة المعقدة لحاكمية الإنترنت بوصفها تتضمن العناصر السياسية التقنية والقانونية والاجتماعية والاقتصادية والعالمية. والشكل الآتي يوضح هذه المجالات.



الشكل (2 ـ 1)

المجالات الرئيسة لانعدام أمن المعلومات

1- جرائم الإنترنت Cybercrime:

ذكر سارق البنوك ويلي ساتون (1901 ـ 1980) انه سرق البنوك لأن المال يوجد هناك. وبما أن المال لا يجسد على شكل آحاد وأصفار في العالم الرقمي، بالتالي فإنه لا ينبغي أن يكون من المستغرب أن الجريمة قد تتبع ذلك في العالم الرقمي. الصك الدولي الوحيد لمعالجة هذا الموضوع هو اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية (2001). وهذه الإتفاقية مفتوحة لجميع الدول الراغبة بالإنصمام لها، وفي أوائل عام 2013، صادقت (39) دولة فقط على الاتفاقية و(10) أخرى وقعت على الاتفاقية ولكنها لم تصادق عليها. (تضم الأمم المتحدة حالياً 193 دولة منضوية كأعضاء).

المبلغ المقدر ـ لكن غير المؤكد عن مبالغ الجريمة الإلكترونية ـ هو مئات المليارات من الدولارات سنويا. فمن المرجح أن بعض الجرائم الإلكترونية لم يبلغ عنها من قبل الضحايا لتفادي تزعزع ثقة الجمهور والمساهمين. مثل هذه الجرائم تتم عبر الحدود ويمكن وضع الحواجز التقنية والقانونية من تعقب واعتقال وتسليم ومحاكمة. الجريمة الإلكترونية تأخذ أشكالا عديدة. من وجهة نظر الشركات، والشكل الرئيسي هي سرقة الملكية الفكرية والإحتيال. وينطبق الشيء نفسه على أشكال أخرى من تسرب البيانات حيث تصل المعلومات الحساسة لأشخاص ليس من المفترض أن يطلعوا عليها. أشكال أخرى من الجريمة الإلكترونية تشمل التخريب و / أو الابتزاز.

الأفراد هم أيضا يمثلون هدفا لجرائم الإنترنت، مثل سرقة الهوية، حيث يمكن لطرف ثالث جمع معلومات كافية عن شخص ليكون قادر على انتحال شخصية (وغالباً إفلاسهم) عن طريق الحصول على الوثائق

والقروض وتفاصيل بطاقات الائتمان. التصيد من أحد الجرائم الإلكترونية ويعني: " استهداف الأفراد (القطاع الخاص و الأفراد) باستخدام الخطابات الإلكترونية والتظاهر بكونهم كيان موثوق به، مثل أحد البنوك، إما للحصول على معلومات شخصية مثل كلمات السر أو تفاصيل بطاقات الائتمان و / أو حملهم على النقر على رابط في الرسالة. هذا الرابط يأخذهم إلى نسخة من موقع موثوق به والذي يطلب منهم تأكيد التفاصيل الشخصية، والنتيجة تكون اصابة أجهزة الكمبيوتر الخاصة بالبرمجيات الخبيثة.

وهناك آخرون بارعون في استخراج المال من ضحاياهم عن طريق الخداع. حيث تتظاهر هذه المجموعة بأنها من أقرباء مسؤول البنك أو الحكومة في بلد بعيد يطلبون المساعدة لنقل مبلغ ضخم من المال، و يطلبون من الضحية دفع رسوم قليلة مقدما لتسهيل عملية تحويل المبلغ. هناك ايضاً الجندي الوحيد (أو العروس البعيدة المحتملة) الذي/التي يحتاج إلى المال للحصول على تذكرة، عملية جراحية، أو غيرها من الاسباب المعقولة، ويطلبون مبلغ بسيط كدفعة وسيتم سدادها في أقرب وقت ممكن. وعلى الرغم من الدعاية التي نتلقاها، إلا أن الضحايا ما زالوا موجودين. وهذه الجريمة ليس من المرجح أن تتوقف في المستقبل القريب.

2- حماية البنية التحتية الحرجة Critical Infrastructure Protection:

هناك العديد من التعريفات للبنية التحتية الحرجة. على سبيل المثال، الشبكة الأوروبية ووكالة أمن المعلومات (ENISA)، وهي جزء من الاتحاد الأوروبي، تصفها على النحو التالي:

تلك النظم والشبكات المترابطة، التي يكون له تأثير خطير على الصحة، والسلامة، والأمن، أو الرفاه الاقتصادي للمواطنين، أو على الأداء الفعال من الحكومة أو الاقتصاد ". الخصائص المحددة والأساسية للبنية التحتية الحرجة هي:

- تعمل (7) أيام في الأسبوع، (24) ساعة في اليوم.
- تتطلب عملياتها نظم المعلومات والشبكات، وأجهزة الاستشعار وغيرها من الآليات للحصول على البيانات.
- تتطلب البنى التحتية الحرجة في كثير من الأحيان تشغيل الأجهزة المادية مثل الصرافات الالية (ATM)، والمحركات (تبديل مسار السكك الحديدية) ونظم الروبوتية (في التصنيع).
- تعد جزءاً من سلسلة التوريد – عليه فإن فشل التشغيل الذي يمتد إلى / من الكيانات الأخرى التي قد تكون أيضا بنى تحتية حرجة، يقود إلى خلق تأثير الدومينو.

وينطبق هذا التعريف على المرافق العامة (الكهرباء، الغاز، والماء)، والنقل (مراقبة الحركة الجوية، وعمليات المطار والسكك الحديدية)، وكل أنواع التصنيع المستمر (مصافي النفط، والزجاج، ومعالجة الورق)، والخدمات المصرفية (ATM الشبكات والانترنت)، والاتصالات السلكية واللاسلكية (الهاتف الثابت والهواتف النقالة، ومقدمي خدمة الإنترنت) وغيرها الكثير. كل هذه هي "غير مرئية" عندما تعمل. وعندما تفشل، فإنها دائما تتصدر عناوين الأخبار.

الهجمات على البنى التحتية الحرجة أصبحت أكثر تعقيداً: وكان حدثا هاما استخدام البرمجية (Stuxnet) لتعطيل مرافق معالجة تخصيب اليورانيوم في ايران، لأول مرة في شهر حزيران من العام (2010). وقد وصف الخبراء (Stuxnet) بأنها "صاروخ أرض ارض الكتروني عسكري. كما أشار خبراء البرمجيات الذين حللوا برمجية (Stuxnet2) إلى ما يلي: "بالتأكيد لم نرى شيئا مثل هذا من قبل". وأكدت مجلة عالم الحاسوب بانها تعد "واحدة من أكثر البرمجيات تطورا وأنها غير عادية من بين البرمجيات التي ظهرت".

ومنذ ذلك الحين كانت هناك هجمات أخرى ناجحة على البنى التحتية الحرجة في كثير من البلدان. ومن بين هذه الهجومات ذلك الذي حصل في أغسطس (2012) كان المستهدف شركة آرامكو السعودية عندما عطل الفيروس شمعون" Shamoon " (30 000) من أجهزة الحاسوب الشخصية، وحذف البيانات الخاصة بها، وتم الاستعاضة عنها بصور لحرق العلم الأمريكي، وبقي مصدر الهجوم مجهول الهوية. الهجوم الإلكتروني واحتمال وجود حرب الكترونية (وهو الحدث الذي لا يوجد تعريف متفق عليه حتى الآن) يمكن القول أن تعرض مشغلي البنى التحتية الحرجة للاضطرابات يعني الفساد أو تدمير البيانات.

3- الأمن والدفاع الوطني National security and defense:

كما هو الحال في اثنين من الأجزاء السابقة، قد تكون الأهداف محددة للغاية، وربما يكون المهاجمون مختلفين. هناك حديث غير مؤكد عن "الجيوش الالكترونية" النشطة في العديد من البلدان. عند مناقشة مثل هذه الأنشطة في الأماكن العامة، يشار إلى أنها تقتصر على "القدرات الدفاعية".

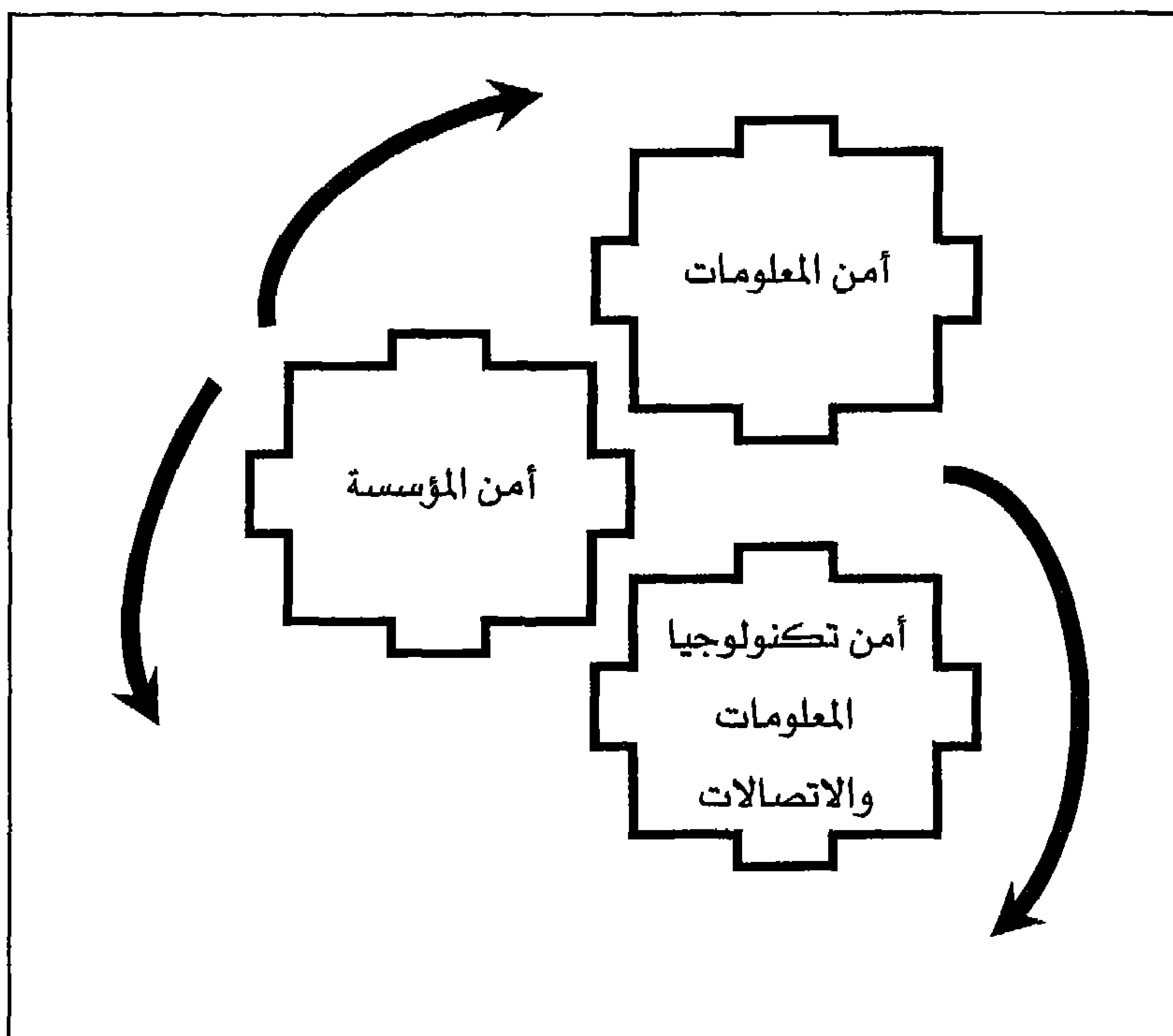
في أكتوبر (2011)، ذكر الجنرال (R. Kehler) من القيادة الاستراتيجية العسكرية للولايات المتحدة ما يلي: "... بحاجة إلى تحديد قواعد الاشتباك لحرب الحاسبة الهجومية".

هناك تكهنات من قبل وسائل الاعلام حول أن القدرات الهجومية هي موجودة بالفعل أو يجري تطويرها في العديد من البلدان. بينما من وجهة نظر أمن المعلومات، فإن المجالات الثلاثة التي نوقشت هنا فيها الكثير من العناصر المشتركة، أحد التحديات العديدة هو عملية انتشار أو عدم انتشار قوانين القتال المسلح مثل (اتفاقيات جنيف و لاهاي) لتشمل الأسلحة الإلكترونية و تحديد ما قد يشكل الأهداف الواجب حمايتها في حالة وجود تعارض إلكتروني. ومع ذلك، فإن المشكلة لن تزول حتى لو يتم تحديث هذه القوانين وتم توقيع معاهدات جديدة، لأن الجهات الفاعلة من غير الدول تتجاهل عمدا الاتفاقيات أو المعاهدات.

رابعاً: الفرق بين الأمن المادي وأمن المعلومات في المؤسسة وأمن تكنولوجيا المعلومات والاتصالات

Differences between Enterprise security, Information security and Information Technology security

تعتمد إدارة أمن المعلومات على ثلاثة مجالات متميزة من المساءلة. وهذه المجالات لا ترتبط دائما مع بعضها بشكل جيد أو يتم تنسيقها على نحو سليم، وفي اغلب الأحيان يتم وضع إدارتها في تشكيلات تنظيمية مختلفة منفصلة ومستقلة بعضها عن البعض الآخر. كما هي موضحة في الشكل (2 ـ 2).



الشكل (2 ـ 2)

مجالات الأمن الرئيسة في المؤسسة

1- المؤسسة والأمن المادي Enterprise and Physical Security:

يتم تعريف الأمن عموما على أنه التحرر من الخطر أو كشرط للسلامة، وينطبق هذا التعريف على أمن الناس، والمباني، ومحتويات المباني، والمنظمات، وحتى الأمم، فضلاً عن المعلومات. ويتم استخدام الأمن في ناحيتين على الأقل:

- الظرف الذي لا ينشأ فيه الأذى، على الرغم من وقوع أحداث تهدد ذلك.
- مجموعة من الإجراءات الوقائية الرامية إلى تحقيق هذا الظرف.

وفقا لذلك، هناك عدد قليل من المنظمات التي ليس لديها شكل ما من أشكال الأمن المادي وشخص مسؤول عن ذلك. وجود موظفي الاستقبال أو الحراس الذين يرتدون الزي الرسمي للتحكم في الوصول هو مألوف للجميع. ولكن السؤال الذي يطرح هنا، هل لدى هؤلاء وزملائهم، والعديد من "وراء الكواليس"، مسؤوليات لأمن المعلومات؟

في الواقع، إنهم يتحملون هذه المسؤولية، جنبا إلى جنب مع وحدات أخرى. هذا يبدأ من التفقد ما قبل الإلتزام والذي تتحقق منه دائرة الموارد البشرية. قد يشمل هذا التحقق الموظفين المحتملين وكذلك الاستشاريين والمدققين الخارجيين والموردين وغيرهم من الزوار. ينبغي التشدد في هذا التحقق والذي يعكس حساسية البيئة الفردية.

الأمن المادي يجب أن يشمل التحقق ومراقبة الصلاحيات المتاحة للوصول إلى المناطق الحساسة والتي يجب أن لا تكون متاحة إلا للأشخاص المصرح لهم بذلك على وجه التحديد. وبالإضافة إلى ذلك، فإنها تتخذ تدابير لضمان أن المعدات والبيانات التي تمتلكها المنظمة لا تتم إزالتها دون وجود صلاحية لذلك، آخذاً بعين الإعتبار الأجهزة الصغيرة)، وأن أي من الأجهزة المفقودة أو المسروقة يتم التعامل معها بشكل مناسب، بما في ذلك إلغاء الصلاحية عن بعد و مسح المحتوى. ويعقب ذلك منح التراخيص، والتي قد تأخذ أشكال مختلفة مثل "الزوار" حيث يتم اصدار شارة مبرمجة مسبقاً لفتح الأبواب و / أو أن تستخدم كرمز للوصول إلى نظام الحاسب.

فريق الأمن المادي هو أيضا مسؤول عن التعامل مع الانتهاكات المشتبه بها أو الفعلية للأمن وهذا يمكن أن يشمل التحقيقات وضبط سلسلة مقبولة

قانونا من الأدلة والاحتفاظ بها، وعند الضرورة جمع كل الوثائق والادلة المملوكة للمنظمة قبل مرافقة الشخص للخروج من المبنى. يتم إخبار قسم الموارد البشرية الذي بدوره يأخذ كل الإجراءات والخطوات الإدارية اللازمة التي تضمن عدم وصول الشخص إلى أنظمة الكمبيوتر والبيانات وإنهاء جميع الإمتيازات والصلاحيات.

2- أمن المعلومات Information Security:

يعد أمن المعلومات النشاط الموزع تنظيميا، وهو النشاط الذي يتعامل مع أصول/ موجودات المعلومات الفعلية للمنظمة، أيا كان الشكل الذي يحفظ فيها (ورقية أو إلكترونية) وحيثما تكون محفوظة (الأرشيف، الحاسبة "سحابة"، في شركة من خلال الاستعانة بمصادر خارجية، منزل الموظف، الخ.).

وشرط السرية يعني أن "المالك" أو "الخادم" للمعلومات هو الجهة الوحيدة بالمعرفة اللازمة لتحديد ما ينبغي أن يكون سري وتحت أي ظروف. وتسمى هذه العملية "تصنيف البيانات". هناك العديد من الطرق المتاحة لتصنيف البيانات، والمنظمات لديها معايير خاصة بها للقيام بذلك. حيث تكون الأمور على ما يرام، طالما يتم تطبيق هذه المعايير بشكل مستمر ومنتظم. الوسيلة السهلة (الكسولة) تقول: "كل شيء سري" ويمكن الوصول إليه فقط من قبل المخولين على وجه التحديد للوصول إلى عنصر معين.

هذا قد يبدو مغريا لكن كمية البيانات التي تحتفظ بها المنظمات ضخمة: الملكية الفكرية والتجارية والتشغيلية والقانونية والمالية، والموارد البشرية، والمشتريات، وأكثر من ذلك بكثير.... في مؤسسة كبيرة، فإن

تحديد حقوق الوصول للأفراد العاملين والحفاظ عليها كلما يحصل هناك تغيير في الوظائف غير واقعي. وعلى الطرف الآخر، هناك أولئك الذين يقولون "نحن فخورون بالشفافية لدينا وليس لدينا ما نخفيه، لذلك لا تصنف أي شيء". هذه هي السذاجة. فكل منظمة، مهما كانت بسيطة أو صغيرة لديها البيانات التي لا ينبغي جعلها مشاعة، على سبيل المثال عنوان ومعلومات البنك للموظف (لأسباب تتعلق بالخصوصية)، وتفاصيل المقترحات التجارية خلال عملية تقديم العطاءات (حساسة تجارياً)، المعلومات السرية ذات القيمة، وغيرها الكثير من المعلومات.

هناك عدة فئات من تصنيف المعلومات تتراوح بين "سري للغاية" و "العامة"، مثل، مقصورة على (مجموعة محددة)، محظور حتى (تاريخ معين)، وما إلى ذلك كل فئة محددة بوضوح وتدعمها قواعد واضحة. التوازن الصحيح بين القيود والانفتاح قد لا يكون واضحا ولكن، وبدون ذلك، فإن المنظمة إما تكون في عقدة أو تكون عرضة للخطر.

هناك تحديات إدارية إضافية: فكل جزء من المنظمة يعتمد على شبكات حاسبات وتطبيقات محددة. إدارة عملية منظمية محددة وأدواتها اللازمة لدعمها تكون مسؤولة عن ضمان حقوق الأفراد في الوصول إلى هذه النظم أو الحصول على "أذونات" تتسق مع أدوارهم ومسؤولياتهم. على سبيل المثال، فإن أحد موظفي البنك العاملين في فرع المحافظات ليس لديه سبب للوصول إلى البيانات عن عملاء في مواقع أخرى. فإذا تم تمكينه من الوصول إلى تلك المعلومات هذا يعني هناك حاجة لتحديد ما هو مسموح للشخص القيام به مع البيانات (للقراءة فقط، تحميل وتحديث، إنشاء، وحذف).

وتعد هذه مهمة شاقة بخاصة عندما لا تدار بشكل مناسب، فقد يؤدي إلى تراكم حقوق الوصول للأفراد (يشار اليها عادة باسم "الأذونات") كلما تحرك الافراد داخل المنظمة نتيجة للترقية أو إعادة التنظيم. وفي الممارسة العملية، فإنه من الصعب إنشاء قائمة مفصلة وكاملة من الأذونات عندما يكون الفرد غير موجود مسبقا. وهناك أدوات يفترض أنها تسهل هذه العملية. وتتضمن نظم المؤسسات الجديدة أدوات لتحديد التحكم في الوصول القائم على الدور(Role Based Access Controls). هذه الضوابط وأي استثناءات مؤقتة لها، تتطلب اهتمام الإدارة والمصادقة العادية عليها.

3- أمن تكنولوجيا المعلومات Information Technology Security:

ويعد المكون الأكثر وضوحا وأيضاً تناولاً في الكتابة، ويعزى ذلك إلى أن البيئة الفنية تتصف بوجود الثقافة الخاصة واللغة الفنية المميزة الخاصة بها. ومن ثم نجد في المنظمة الأنشطة الضرورية لحماية المعلومات من الوصول غير المصرح به والتعديل عليها، ولكن هذه الأنشطة قد لا تتواجد في كل المنظمات، كما هو الحال عندما يتم توفير عمليات وخدمات تكنولوجيا المعلومات من خلال المزود (المورد) الخارجي في إطارما يصطلح عليه الاستعانة بالمصادر الخارجية (Outsourcing). مثل هؤلاء الموردين عادة ما يقدمون الخدمة بالاستعانة بمصادر خارجية، وصيغة التعاقد، وخدمات الطرف الثالث (rd3)، والموظفين المؤقتين وغيرها من السمات التي تميز هذا النوع من خدمات تكنولوجيا المعلومات والاتصالات. ومن المعتاد أن نجد مدير أمن المعلومات في قسم تكنولوجيا المعلومات الذي يعمل في إطارأهداف معروفة

ومهام محددة بشكل واضح مع كافة الصلاحيات والمسؤوليات التي تمكنه من القيام بواجباته على نحو سليم.

4- أهمية إدارة أمن المعلومات:

Information security is increasingly important

تتبع أهمية إدارة أمن المعلومات من أهمية الهدف الذي تسعى هذه الادارة إلى تحقيقه والمتمثل في توفير الحماية الحكيمة للمعلومات من الضياع تماماً مثلما يتم حماية أي أصول/موجودات أخرى ذات قيمة، مثل الممتلكات المادية، والمعدات، والمال، أو الموظفين عن طريق استخدام الضوابط الأمنية والممارسات التي يتطلبها تنفيذ وتلبية معيار العناية الواجبة سواء من قبل الفرد أو المنظمة، فإدارة أمن المعلومات أمر ضروري لأسباب مختلفة، بعضها يكون مطلوباً لمنع وقوع أي حوادث أمنية، لمنع وقوع وللكشف عن أي من تلك الأحداث. والسؤال الذي يطرح هنا هو: لماذا تتزايد أهمية إدارة أمن المعلومات؟

للاجابة عن هذا السؤال، يشير الخبراء إلى أن إدارة أمن المعلومات توفر للمنظمة استراتيجية مختصرة ولكنها عالية المستوى وشاملة لصياغة الحلول الأمنية التكتيكية ذات العلاقة بأهداف المنظمة. وعلاوة على ذلك، فإنه يحدد بوضوح قيمة أصول/موجودات المعلومات، تجسد أولويات المنظمة الواسعة، و تقررنهائيا متطلبات العمل والافتراضات التي تسير وتقود أنشطة الأمن. وعند قيام إدارة المنظمة بعملية تطوير إدارة أمن المعلومات ذات الصلة على نحو سليم، يمكن للمنظمة اتخاذ القرار الصعب بشأن برنامج أمن المعلومات على مستوى الادارة العليا، الأمرالذي يجعل تنفيذ بقية البرنامج أسهل من ذلك بكثير. وبالإضافة إلى ذلك، فإن المنظمة التي تقوم بمراجعة

وتقويم تنفيذ سياستها الحالية في أمن المعلومات بانتظام يمكنها تحديد النقائص الرئيسية و العناصر غير الفعالة ضمن برنامجها لأمن المعلومات.

من جهة أخرى وبوساطة الاسترشاد بأفضل ممارسة لإدارة أمن المعلومات، يمكن للمؤسسة تقييم وتحسين أو تطوير سياسة أمن المعلومات الخاصة بها، و تعزيز التواصل بين أعضاء فرق أمن المعلومات و الإدارة التنفيذية وإدارات وحدة الأعمال. كما أنه يمكن أيضا أن يوفر فهماً مشتركاً للأسس اللازمة لأمن المعلومات أكثر فعالية.

- طالما أن المنظمات تعتمد على تكنولوجيا المعلومات وأنظمة تكنولوجيا المعلومات في معالجة البيانات وتخزين المعلومات و نقلها و تنظيم بيانات العملاء، ونتيجة لذلك، فإنه في حالة حدوث فشل نظام تكنولوجيا المعلومات، سواء كان ذلك من خلال حدث خبيث أو تقني من حوادث فشل النظام أو فقدان المعلومات، فإنه سيكون غير المجدي استخدام المعالجة اليدوية كبديل أو كحل للمشاكل.
- هناك أيضا عددا من القضايا الأمنية المحيطة بأمن المعلومات، مثل تزايد حركية المنظمات (mobility) التي أتاحت المجال للوصول اليها عن بعد لاسلكياً من خلال شبكة الانترنت.
- قيمة أجهزة الحاسوب وملحاقاتها المادية قد تكون مقدرة بالآلاف من الدولارات، ولكن المعلومات التي تتضمنها هذه الأجهزة، قد تكون قيمتها مقدرة بأكثر من الملايين من الدولارات.
- وبينما هناك حاجة لأنظمة حاسبات موثوقة توفر الأمن والخصوصية للشركات والمستهلكين على حد سواء، فإن هناك ثمة حاجة أيضا

للمهنيين في أمن الأنظمة والذين يقدمون المساعدة في تصميم وتكوين وتنفيذ وإدارة ودعم و تأمين هذه النظم الحاسوبية. بتعبير آخر يعد الموظفون الذين يمتلكون المعرفة بأمن نظم المعلومات في عصرنا الحالي جزءا هاما من بين العديد من فرق البنية التحتية لتكنولوجيا المعلومات.

- من الضروري أن يصبح أمن تكنولوجيا المعلومات جزءا لا يتجزأ من نشاط المنظمة بحيث إذا كان لكل قسم سياسته الخاصة بتكنولوجيا المعلومات، والتي - وإلى حد ما - تختلف عن بعضها البعض، فمن المحتمل جداً أن الاختراقات سوف تترتب على ذلك.
- سلسلة القيمة لإدارة أمن المعلومات. تعرف إدارة أمن المعلومات المعلومات كأصل/موجود يضيف قيمة إلى المنظمة ويحتاج بالتالي إلى توفير الحماية المناسبة لها. وتشمل إدارة أمن المعلومات عددا من العمليات المنظمية المنفصلة التي تجمع بين مخاطر الحوادث، الجريمة، والاستخدام غير الفعال. لذلك هناك بعض المخاطر العامة المرتبطة بالاختراق الأمني مثل فقدان الدخل (تقليل العائد على الاستثمار)، ومزايا تنافسية (فرص العمل) والعقوبات القانونية على المنظمة.
- تشير نتائج الخبرة الميدانية بخصوص تكامل التدابير الأمنية إلى أن إدراج هذه التدابير في مرحلة تصميم النظام هو أقل كلفة بكثير من تحسين هذه التدابيرعلى النظام القائم. وتظهر التكاليف النسبية لإدماج تدابير أمنية في مراحل مختلفة من تطوير النظام

وتشغيله. وتستمد هذه البيانات من التكاليف الفعلية لإجراء التغييرات على البرمجية في نقاط مختلفة من تطوير النظام، وهي تختلف بمعامل أكثر من (200٪) في مرحلة التصميم.

- النمو المستمر لسوق أمن المعلومات، إذ لا يزال هذا السوق في طور النمو طالما أن المجهزين لمنتج الأمن يسعون جاهدين لمواكبة المشاكل الجديدة لأمن المعلومات. ويركز العديد من هؤلاء المجهزون على توفير التكنولوجيات لحل مشاكل أمنية معروفة. على سبيل المثال، في التحكم في الوصول إلى الشبكات الداخلية للشركة، هناك جدران الحماية، ولرصد حالات التسلل الممكنة، هناك أنظمة كشف التسلل (IDSs)؛ لتحليل حزم البيانات المنقولة من وإلى الشبكات، وهناك (snuffers)؛ للتخفيف من مخاطر فيروس الهجمات، وهناك برامج مكافحة الفيروسات.

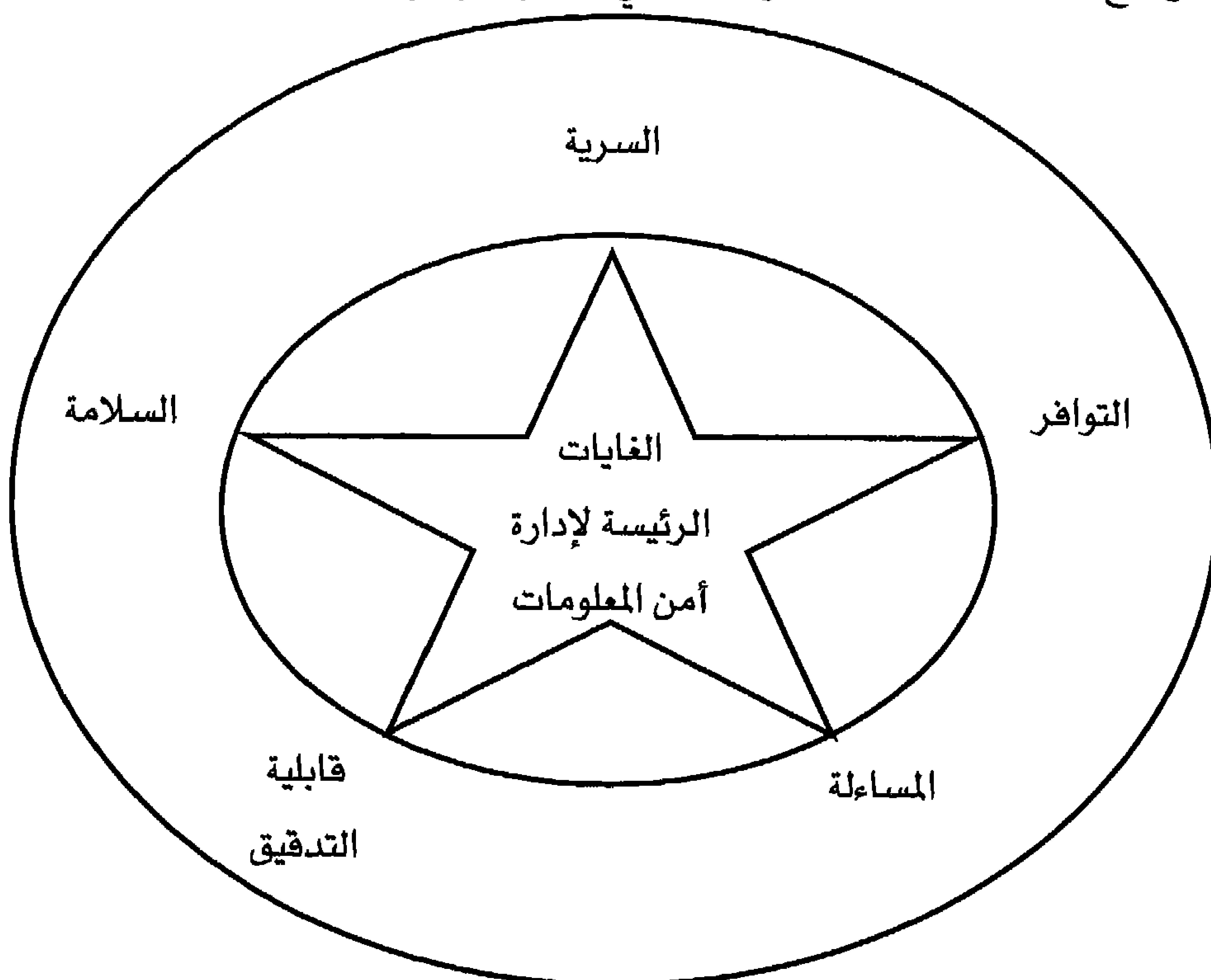
خامساً: غايات إدارة أمن المعلومات Information Security Targets

لقد أصبحت إدارة أمن المعلومات مهمة صعبة ومعقدة على نحو متزايد وتشكل تحديا كبيراً، حيث أسهم التقدم الهائل في مجال الحوسبة وتكنولوجيا المعلومات والاتصالات خلال السنوات الخمس الماضية في إعادة توجيه التركيز في معالجة البيانات من مركز الحاسبة إلى المحطات الطرفية (النهايات) في المكاتب والمنازل الفردية. والنتيجة هي أن المديرين يجب عليهم الآن رصد الأمن على مستوى أكثر إنتشاراً وعلى نطاق واسع. وتتواصل هذه التغيرات بشكل متسارع، مما يجعل وظيفة مدير الأمن معقدة على نحو متزايد. بناءاً عليه يجب على مدير أمن المعلومات إعداد برنامج الأمن على

النحــو الــذي يــضمن تحقيــق ثلاثــة غايــات جوهريــة هــي: الــسرية (Confidentiality) والــسلامة (Integrity) وتــوافر مــوارد المعلومــات (Availability) في المنظمـة. وتنعكس هـذه الغيـات في معيـار (27000 ISO) الـدولي، ويستخدم علـى نطـاق واسـع. وقـد اقترح الممارسين الأمنيين غايـات إضافية. في عام (2002)، اقترح (D.B. Parker) ثلاثة غايات إضافية هـي:

- الأصــالة (Authenticity)، وتعــني التأكــد مــن أن الأطــراف في المعاملـة الإلكترونيـة هـم نفـسهم الـذين يـدعون أنهـم المتعـاملون الاصلاء، وأن مكونات هذه الصفقة هي حقيقية.
- الحيازة والتحكم، وتعني امتلاك المعلومات والتحكم بهـا في ظل ظروف معينة، ويحصل اختراق أمن الحيازة من الحصول علـى نسخ مـن المعلومـات أو التخلـي عـن رقابتهـا او الائتمـان عليهـا. عليـه فـأن خسارة الإستحواذ على البيانات والتحكم بهـا تخلق خطـر فقـدان أمن المعلومات. مثال على ذلك، جهاز حاسب محمول منسي ولم يتم انتشاله عند نقطة أمن المطار.
- الفائدة (المنفعة Utility)، تشير إلى حالـة المعلومـات الـتي تعـد مفيـدة أو متطابقة مع هدف محدد ومن ثم القدرة على استخدام المعلومـات. على سبيل المثال، افترض أنـه تم توفير البيانـات المشفرة للفـرد جنبـا إلى جنب مع مفتاح التشفير ولكن المتلقي فقد مفتاح التشفير. تبقـى البيانات المتاحة، أصيلة وسـرية، فإنهـا تحـتفظ بـسلامتها الأصـلية، وهــي في حــوزة الـشخص المقـصود. ولكــن لأنهــا ليـست صـالحة للاستعمال فإنها ليست نافعة.

من جهة أخرى أضافت أدبيات وتطبيقات التجارة الإلكترونية غاية إضافية جديدة هي: عدم التنصل ويشير إلى الآلية التي تضمن أن طرفا في الصفقة لا يمكنه أن ينكر أنه تلقى المعاملة، ولا يستطيع الطرف الآخرأن ينكر أنه أرسل تلك الرسالة. بينما يرى خبراء آخرون أن يشمل النموذج الأمني الأساسي غايات السرية والسلامة والتوافر، إلى جانب إضافة غايتين هما المساءلة (Accountability) و قابلية التدقيق(Audit ability). كما هو موضح في الشكل (2 ـ 3). وفيما يأتي فكرة موجزة عن هذه الغايات.



الشكل (2 ـ 3)

الغايات الرئيسة لأمن المعلومات في أية منظمة

1- السرية (Confidentiality):

تشير السرية إلى الصفة الخارجية التي تمنح للمعلومات والتي تنطوي على التكتم والخصوصية وذلك من خلال تحديد الضوابط والتعليمات التي تحدد الجهات المسموح لها بالاطلاع عليها ومن ثم حماية المعلومات في النظام بحيث لا يمكن للأشخاص غير المرخص لهم الوصول إليها. أي تأمين تدفق المعلومات في القنوات المخصصة لها ومنع تسربها خارج هذه القنوات بالشكل الذي ينعكس سلباً على حاكمية أمن المعلومات. إذ تعد مسألة تحقيق السرية من المهام الحساسة جداً والمثيرة للقلق والإزعاج في أن واحد لإدارات المنظمات، نظراً للأضرار التي يمكن أن تلحق بها بخاصة عند تسرب المعلومات الحساسة وخاصة الاستراتيجية منها على قدرة المنظمة في تحقيق ميزات استراتيجية.

بتعبير آخر يتم تحقيق هذه الغاية (المحافظة على السرية) من خلال التأكد من أن المعلومات يمكن الوصول إليها فقط من قبل أولئك المخولين للقيام بذلك، عليه يحصل الاختراق في السرية في إمكانية الوصول إلى المعلومات والكشف عنها أو مراقبتها. ويعتقد الكثير أن هذا النوع من الحماية هو الأكثر أهمية للمنظمات العسكرية و الحكومية التي بحاجة للحفاظ على الخطط و القدرات السرية من الأعداء المحتملين. ومع ذلك، فإنها يمكن أيضا أن تكون مهمة للشركات التي تحتاج إلى حماية الأسرار التجارية الخاصة بها من المنافسين أو منع الأشخاص غير المرخص لهم من الوصول إلى المعلومات الحساسة للشركة (على سبيل المثال، القانونية، الموظفين، أو المعلومات الطبية). قضايا الخصوصية، التي نالت قدرا متزايدا

من الاهتمام في السنوات القليلة الماضية، تبرز أهمية السرية على حماية المعلومات الشخصية المحفوظة في النظم المؤتمتة من قبل كل من الوكالات الحكومية و منظمات القطاع الخاص. السرية يجب أن تكون محددة بشكل جيد، كما يجب أن تنفذ إجراءات الحفاظ على السرية بعناية فائقة، وخاصة بالنسبة للحاسبات المستقلة. وأحد الجوانب الحاسمة من السرية هو تعريف المستخدم (تحديد هويته) والمصادقة(منحه التخويل). التحديد السليم لهوية كل مستخدم للنظام أمر أساسي لضمان فاعلية السياسات التي تحدد من يسمح له بالوصول إلى أي من مفردات البيانات.

2- توافر المعلومات (Availability):

تعني ضمان توافرالمعلومات للأطراف المخولين بالوصول إلى المعلومات عند الحاجة. وتتحقق هذه الغاية عند امتلاك تلك الاطراف المخولة القدرة على الوصول إلى المعلومات وإمكانية استخدامها بصورتها الحالية أينما كانت وكيفما تطلب الأمر، ويحصل الاختراق لأمن المعلومات عند تخريب المعلومات أو اختلاطها بمعلومات أخرى ـ على النحو الذي يؤدي إلى تلوثها ـ أو رفضها أو تأخير وإطالة استخدامها أو سوء تفسيرها أو قلبها. بتعبير آخرتكون البيانات مفيدة فقط عندما يتمكن الأفراد من الوصول إليها. وسهولة الوصول تعني المدى الذي يكن للمستفيد الحصول على البيانات في الوقت الملائم لاستخدامها على نحو فاعل وبالشكل الذي يجعلها مفيدة. ويستند الوصول إلى البيانات على قدرة المستفيدين من البيانات على تحديد قيمة الانواع المختلفة من البيانات الموجودة. ومن خلال تكامل جهود تقييم المخاطر مع الاجراءات القانونية والتنظيمية المعتمدة في التحكم بالوصول إلى البيانات

(مثل متطلبات قانون" Graham-Leach Bliley " للمؤسسات المالية)، فإن معايير الصناعة سوف تخدم بمثابة دليل لكتابة وتحديث السياسات والمعايير الخاصة بالوصول إلى البيانات في المنظمة. وهناك العديد من العوامل التي تحدد الطريقة التي تخزن فيها المعلومات والطريقة التي يرغب بها المستفيد في عرض المعلومات، عليه فان مهارة المستفيد في إيجاد المعلومات التي يحتاجها هي التي تؤثر في سهولة الوصول اليها. على سبيل المثال المعلومات المخزونة في قاعدة معلومات مشتركة قد يصعب الوصول إليها بالوقت المناسب بالمقارنة مع تلك المخزونة في الحاسب الشخصي للمستفيد.وبشكل عام فان استخدام التخزين الإلكتروني بدلاً من الورقيات جعلت المعلومات أكثر سهولة في الوصول. ويمكن أن تستند معايير الوصول إلى البيانات على تعريف الاستخدام "غير المقبول" للبيانات والمتطلبات الخارجية لإمكانية التدقيق (القدرة على تتبع من / ما هي البيانات التي تم الوصول اليها / تعديل البيانات). من جهة ثانية تسهم قرارات الوصول إلى البيانات أيضا في توفير المعايير على المستويين المادي والمنطقي (Pfleeger, C. P. and Pfleeger و2003).

3- **تمامية/ سلامة المعلومات** (Integrity):

تتضمن التمامية الصفات الجوهرية الخاصة بكمال المعلومات وتماسكها وارتباطها بمجموعة القيم السائدة في المنظمة، وتتحقق هذه الغاية عند الحفاظ على دقة واكتمال المعلومات وإتصافها بالصدق والأصالة وعمق تطابقها مع الحقيقة والواقع وضمان أنه لم يتم إجراء أية تغييرات غير مصرح بها على هذه المعلومات. أي أن هذه الغاية يجب أن تشتمل على كلا المعيارين وهما معايير السلامة المادية ومعاييرالسلامة المنطقية، إذ تهدف معايير

السلامة المادية للبيانات إلى التأكد من أن البيانات محصنة ضد الأذى المادي مثل انقطاع الكهرباء، بينما تهدف معايير السلامة المنطقية للبيانات إلى ضمان الحفاظ على بنية وهيكلية قاعدة البيانات ومحتوياتها من المعلومات. من هنا يحصل الاختراق لأمن المعلومات في إطار هذه الغاية عند إدخال أو استخدام أو خلق معلومات كاذبة أو تحوير أو استبدال المعلومات أو سوء تفسيرها أو سوء استخدامها أو الفشل في استخدامها.

4- المساءلة (Accountability):

يعد مفهوم المساءلة من المفاهيم المتجددة إذ تختلف دلالاته تبعاً لمقاصده، وفي مجال أمن المعلومات تعني المساءلة تحمل الشخص الذي قام بالوصول إلى أي معلومة داخل النظام، مسؤولية التغيير الذي حدث عليها أثناء وصوله اليها سواء كان موظفاً مسؤولاً عن معالجة المعلومات أو أحد العملاء وهذا الإجراء يتضمن تحمل المسؤولية لكل الأفراد الذين يستطيعون الوصول للمعلومة ويمتلكون الصلاحيات بتغيير المعلومات أو حتى الوصول إلى المعلومات. وتتحقق هذه الغاية عندما يتم ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها، إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفرالقدرة لإثبات أن تصرفا ما قد تم من شخص ما في وقت معين". ولأجل إقرار المساءلة يشترط المتخصصون في أمن المعلومات ضرورة الالتزام بمجموعة من المبادئ التي يمكن اختصارها في الآتي:

- وضوح قواعد النظام وعواقب المخالفات: يجب أن يدرك العاملون بوضوح القواعد المطلوب الالتزم بها وعواقب مخالفتها، وأن توضح الفائدة من التمسك بتلك القواعد.

- مبدأ المباشرة في تطبيق الجزاء: إيجاد ارتباط بين المخالفة وبين الجزاء حتى يتجنبه العامل مستقبلاً، ويجب أن يكون هنالك تحقيق كامل للمخالفة وأسبابها.
- عدالة تطبيق الجزاء: يجب أن يقتنع العاملون بعدالة تطبيق الجزاءات حتى يتقبلوها، لذلك يجب أن يكون هناك تحذير واضح بأن مخالفة معينه تعرض من يرتكبها لجزاء معين.
- المساءلة والتجانس في توقيع العقوبة: يعد هذا المبدأ من أهم مبادئ المساءلة ويجب أن يفهم أن العقوبة لا ترتبط بالشخص المخالف ولكن ترتبط بنوع المخالفة، وإذا ارتكب عاملان المخالفة نفسها وعاقب المدير عاملاً وترك الآخر فإن إدارته تتهم بالتحيز والمحاباة.
- مبدأ التدرج في شدة العقاب: يجب أن يكون هناك نوع من التدرج في نوع العقوبة بما يتناسب مع نوع المخالفة وتكرارها.

5- قابلية التدقيق (Audit ability):

وتسمى أيضا المصداقية وتشير إلى عملية التقييم لحالة أمن المعلومات في المنظمة مقارنة بمستوى العمل القياسي فيها، وضمان أن الموظفين يتصرفون وفقاً للإجراءات المتبعة والمبادئ التوجيهية التي يمكن استخدامها لتعزيز حالة الامن. والتدقيق على البيانات الموجودة داخل الحاسبات، ومتابعة عمل الموظفين الذين يعملون على أنظمة المعلومات الموجودة. وتتحقق هذه الغاية عندما يتم التأكد من أن مقاييس أمن المعلومات مقبولة في إطار تطبيقات نظم المعلومات. ومعرفة مدى تجاوز المستخدم التخويل أو التصريح الممنوح له، إلى جانب التأكد من صحة البيانات والمعاملات، والإتصالات والوثائق بغض

النظرعما إذا كانت (إلكترونية أو تقليدية) وأيضاً التحقق من صحة جميع الأطراف المعنية بالأنظمة. ويشير بعض المتخصصين إلى أن هذه الغاية تأتي في النهاية لضمان أن كل الغايات السابقة تم تحقيقها بشكل صحيح.

أسئلة الفصل

س (1): عرف أمن المعلومات:

- بشكل عام
- من وجهة النظر القانونية

من وجهة نظر التقنية العامة

س (2): يميل معظم تعاريف أمن المعلومات إلى التركيز على وسيلة محددة أو إستخدام محدد وهو إعتقاد خاطئ، لماذا؟

س (3): يجب أن يهتم أمن المعلومات بتحقيق أمن كافة موارد المعلومات في المنظمة، ما هو رأيك؟

س (4): أمن المعلومات هو بطبيعته و بالضرورة، ليس بالمحكم ولا بالمانع الذي لا لبس فيه ولم يبلغ حد الكمال، هل تؤيد هذه المقولة، ولماذا؟

س (5): تتباين الجوانب التي تثير الاهتمام لاختراق أمن المعلومات بتباين طبيعة المعلومات التي تكون عرضة للاختراق، علق على العبارة من خلال عرض بعض الأمثلة.

س (6): وضح من خلال الجدول أهم مراحل تطور مفهوم أمن المعلومات.

س (7): وضح من خلال الشكل أهم مجالات إنعدام أمن المعلومات.

س (8): الأفراد هم أيضا يمثلون هدفا لجرائم الإنترنت، كيف يحصل ذلك؟

س (9): بعض الجهات بارعة في استخراج المال من ضحاياها عن طريق الخداع. كيف يحصل ذلك؟

س (**10**): عرف البنية التحتية لأمن المعلومات.

س (**11**): يؤكد المتخصصون على حقيقة أن الهجمات على البنية التحتية لأمن المعلومات أصبحت في عصرنا الحاضر أكثر تعقيداً، لماذا؟

س (**12**): وضح طبيعة العلاقة بين أمن المعلومات والأمن والدفاع الوطني.

س (**13**): يشير المتخصصون إلى ضرورة التمييز بين موضوعات أمن المؤسسة وأمن المعلومات وأمن تكنولوجيا المعلومات والاتصالات، ماذا تقترح؟

س (**14**): وضح من خلال الشكل الغايات الاساسية لأمن المعلومات.

س (**15**): ضع دائرة أمام الإجابة المناسبة:

تحقيق غايات أمن المعلومات يعتمد على:

A- المعلومات محل الحماية	B- إستخدامات هذه المعلومات
C- الخدمات المتصلة بالمعلومات	D- جميع ماذكر صحيح

س (**16**): عرف سرية المعلومات.

س (**17**): يؤكد المتخصصون على أنه ليس كل أنواع المعلومات في المنظمة تتطلب السرية، لماذا؟ علل.

س (**18**): عدد اهم الجوانب التي تركز عليها غاية سرية المعلومات.

س (**19**): عرف الاتاحية (التوافر).

س (**20**): عدد اهم الجوانب التي تركز عليها غاية إتاحية المعلومات.

س (**21**): يؤكد المتخصصون على أنه غاية إتاحية المعلومات تعد من أهم غايات أمن المعلومات، لماذا؟ علل.

س (**22**): عرف تمامية (سلامة) المعلومات.

س (**23**): ضع دائرة أمام الاجابة المناسبة:

تعني تمامية (سلامة) المعلومات:

A- جودة المعلومات (تكون صحيحة ودقيقة)	B- تكلفة المعلومات(تكون منخفضة التكلفة)
C- اسلوب الحصول على المعلومات	D- جميع ماذكر صحيح

س (24): ضع دائرة أمام الإجابة المناسبة:

يحصل الاختراق لتمامية (سلامة) المعلومات عندما يتم:

A- إستخدام أو إدخال معلومات كاذبة	B- تحويرأو استبدال المعلومات
C- سوء تفسير المعلومات او سوء إستخدامها	D- جميع ماذكر صحيح

س (25): عرف المساءلة.

س (26): وضح باختصار أهم المبادئ التي يجب الالتزام بها عند تحقيق غاية المساءلة لأمن المعلومات.

س (27): عرف قابلية التطبيق.

س (28): أجب بوضع إشارة (صح) أو إشارة (خطأ) أمام العبارات الآتية:

	العبارات	الاشارة
1	" لا يزال سوق منتجات أمن المعلومات في طور النمو طالما أن المجهزين لمنتج الأمن يسعون جاهدين لمواكبة المشاكل الجديدة لأمن المعلومات.	
2	في حالة فشل نظام تكنولوجيا المعلومات والاتصالات،	

	فإنه سيكون من المجدي استخدام المعالجة اليدوية كبديل أو كحل للمشاكل.	
3	قيمة أجهزة الحاسوب وملحاقاتها المادية قد تكون مقدرة بالآلاف من الدولارات، ولكن المعلومات التي تتضمنها هذه الأجهزة، قد تكون قيمتها مقدرة بأكثر من الملايين من الدولارات.	
4	تزايد حركية المنظمات ليست لها علاقة بزيادة الاهتمام بأمن المعلومات	
5	يعد الموظفون الذين يمتلكون المعرفة بأمن نظم المعلومات في عصرنا الحالي جزءا هاما من بين العديد من فرق البنية التحتية لتكنولوجيا المعلومات والاتصالات.	
6	لا يعد أمن تكنولوجيا المعلومات والاتصالات جزءاً من نشاط المنظمة	
7	سلسلة القيمة لإدارة أمن المعلومات. ترتبط باعتبار المعلومات كأصل/موجود يضيف قيمة إلى المنظمة	
8	تكون تكاليف أمن المعلومات في مرحلة التطبيق أعلى منها في مرحلة التصميم	

الفصل الثالث

حاكمية أمن المعلومات

3 

- تمهيد
- أولاً: الغرض من حاكمية أمن المعلومات
- ثانياً: مكونات حاكمية أمن المعلومات
- ثالثاً: مبادئ حاكمية أمن المعلومات
- رابعاً: قواعد السلوك/ المعايير لأمن المعلومات

الفصل الثالث

حاكمية أمن المعلومات

Information Security Governance

تمهيد:

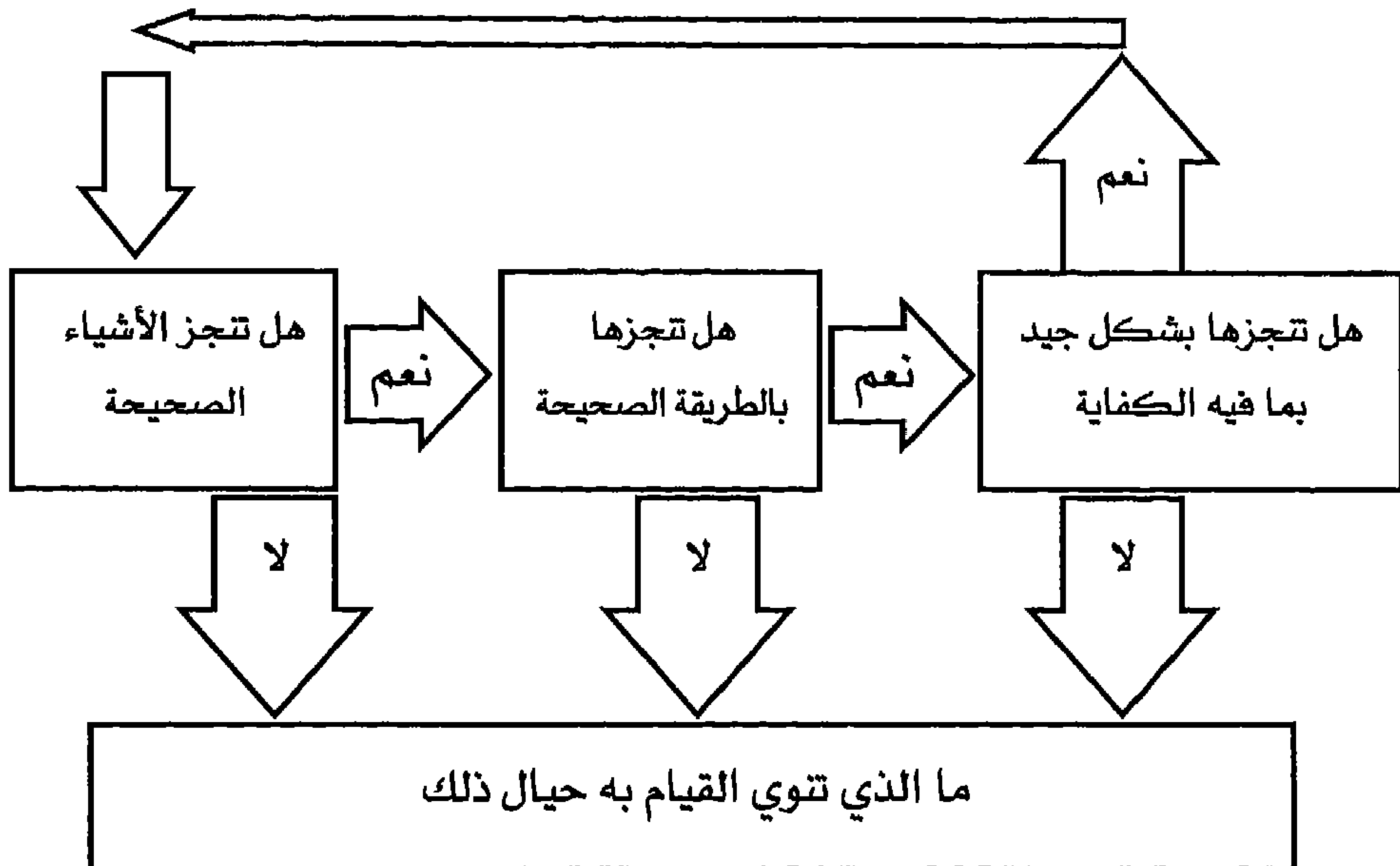
يشير الباحث ((Pierre Van Beneden,(2011)) إلى أنه في بيئة الأعمال اليوم، فان الهفوات التي ترتكبها المنظمات في إدارة الأعمال ذات الصلة بالمعلومات تكلف المنظمة الملايين من الدولارات فضلاً عن الأضرار قد تصيب صورة العلامة التجارية. وتعد حاكمية أمن المعلومات وسيلة مهمة في هذا المجال لانها ستسهم في التخفيف من المخاطر وخفض التكاليف وضمان التعامل مع الموارد / الأصول المعلوماتية في المدى الطويل بطريقة نظامية متوافقة ومستدامة واقتصادية. وتفرض حاكمية أمن المعلومات سلوكية مرغوبة للتعامل مع مختلف أنشطة ادارة المعلومات على مستوى المنظمة ككل وعبر تشكيلاته المختلفة. وبتعبير أخر تحدد حاكمية أمن المعلومات معايير إدارة المعلومات من قبل المنظمة، وتضمن التزامها بمجموعة كبيرة من الأنظمة العالمية والمحلية. فهي أكثر من مجرد وسيلة لإدارة السجلات والاحتفاظ بها والتصرف فيها (إدارة السجلات التقليدية)، فهي تمثل برنامجاً تشمل العمليات المنظمية والممارسات ذات العلاقة بدورة حياة المعلومات. إنها تشتمل على سمات خصوصية البيانات، ومتطلبات تحسين تخزين وإدارة البيانات وسلامتها وإتاحتها.

أولاً: الغرض من حاكمية أمن المعلومات (ISG)

تهدف حاكمية أمن المعلومات إلى تقييم وتوجيه ومراقبة الإجراءات المتخذة لتلبية احتياجات المنظمة لأمن المعلومات وكيفية تنفيذ هذه

الاجراءات. وصولاً إلى تقليل مخاطرالأعمال المتعلقة بالاضطراب التشغيلي، وفقدان المعلومات الحساسة، والتعامل مع حالات عدم الامتثال للمتطلبات التنظيمية والقانونية ذات الصلة بأمن المعلومات إلى جانب تعزيز ثقافة المساءلة عن البيانات وتحديد الادوار والمسؤوليات. من هنا ولاجل تحقيق هذا الهدف لابد على الجهات المسؤولة عن إدارة أمن المعلومات تهيأة الاجابة (وباستمرار) عن التساؤلات الثلاثة الاتية الموضحة في الشكل (3 ـ 1):

- هل تنجز إدارة أمن المعلومات الأمور بشكل صحيح؟
- هل تفعل إدارة أمن المعلومات الأشياء الصحيحة بالطريقة الصحيحة؟
- هل تفعل إدارة أمن المعلومات الأشياء الصحيحة بالطريقة الصحيحة جيدا بما فيه الكفاية؟



الشكل (3 ـ 1)

التساؤلات الثلاثة لادارة أمن المعلومات

1- هل تنجز إدارة أمن المعلومات الأمور بشكل صحيح؟

Are you doing the right things?

تشمل "الأمور في نصابها الصحيح" مواضيع مثل:

- وجود آلية فعالة لحاكمية أمن المعلومات.
- تبني وتطبيق المعايير والمبادئ التوجيهية والممارسات الجيدة.
- وجـود تعريفـات واضـحة للأهـداف والغايـات ومصادر المساءلات، والقياسات، وما إلى ذلك.
- وجود سياسات أمنية واضحة وقابلة للتنفيذ.
- وضع برنامج للإحاطة والتدريب على أمن المعلومات.

إذا كان الجواب على هذا السؤال (هل تنجز إدارة أمن المعلومات الأمور بشكل صحيح) هو (لا)، فإن المنظمة معرضة للخطر. وفي أحسن الأحوال، فإن الافراد سوف يحتاجون إلى تخمين ما هو متوقع منهم و / أو ليس لديهم المهارات أو الموارد اللازمة للقيام بعملهم.

2- هل تفعل إدارة أمن المعلومات الأشياء الصحيحة بالطريقة الصحيحة؟

Are you doing the right things the right way?

بدلا من إعداد وكتابة سياساتهم الأمنية (ليست مهمة تافهة) هناك أولئك الذين يختارون طريقة أسهل للقيام بذلك: شراء قوالب قياسية لمثل هذه الوثائق، والقيام بعملية بحث سريعة واستبدال، وطباعة الوثائق ووضعها في خزانة الملفات. وهذا يخلق الاعتقاد بأنه"تم الانجاز ". يعد هذا النهج بعيدا عن كونه ممارسة جيدة. وينطبق الشيء نفسه على الخبراء الاستشاريين للقيام

بذلك دون مشاركة والتزام من قبل القوى العاملة. الاستشاريين يمكنهم إضافة القيمة من خلال تجربتهم ولكنهم، في نهاية المهمة، سوف يتركون المنظمة للذهاب إلى عميل آخر. بعد ذهابهم، لا أحد في المنظمة سوف يشعر بملكية هذا العمل. في نهاية المطاف هذا الجهد سينتهي مرة أخرى في خزانة الملفات.

وهناك غيرها من الأنشطة التي تحتاج إلى القيام بها في "الطريق الصحيح" بشكل موازي مع المعايير والممارسات الجيدة المختارة. وتتأثر هذه الخيارات بالثقافات الوطنية والتنظيمية، ومتطلبات الحكومة والضوابط، والممارسات المفضلة من مقدمي الخدمات، والمتعاقدين الخارجيين والممارسين في المنظمة. إذا كان الجواب على هذا السؤال هو (لا)، سيكون من الجيد استكشاف لماذا (لا). أسباب كثيرة يمكن أن نتصورها مثل: ضيق الوقت، ونقص التمويل، والافتقار إلى المعرفة، والغطرسة التقنية ("نحن نعرف أفضل")، وعدم الوضوح فيما يتعلق بمن يصنع هذه القرارات... الخ.

3- هل تفعل إدارة أمن المعلومات الأشياء الصحيحة بالطريقة الصحيحة جيدا بما فيه الكفاية؟

Are you doing the right things the right way well enough?

فمن الممكن أن تكون الإجابة على السؤالين السابقين (نعم) وهذا شيء جيد. ومع ذلك، فعل تلك الاشياء جيدا بما فيه الكفاية يتطلب المعرفة والتفاني والانضباط ومشاركة الموظفين. عند فقدان أي من هذه المتطلبات الأربعة، سيتم تنفيذ المهام بطريقة غير مرضية وتكون مدعومة بوساطة الأعذار: "آسف، لم يكن لدي الوقت للقيام بالحفظ الاحتياطي للبيانات لهذا

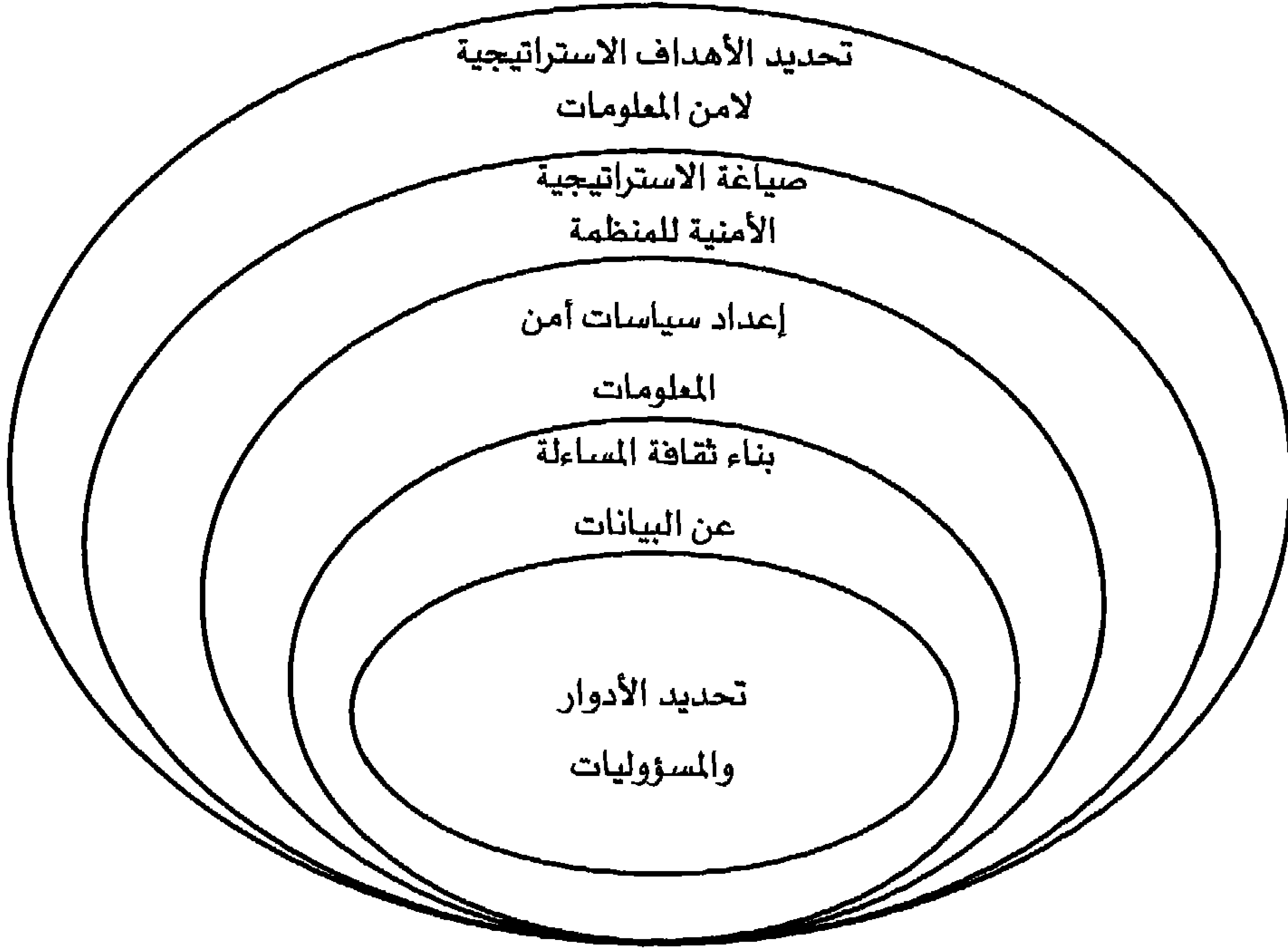
النظام الهام وتم فقدان البيانات الآن"، أو "عذرا، لم نفعل الاختبار على هذا التعديل وأنا واثق من أنه سيكون(OK)"(تخمين ما: لم يكن). إذا كان الجواب على هذا السؤال هو (لا)، فإن المنظمة تواجه مشكلة إدارية قد تتطلب حقن التحفيز، التدريب، والتوظيف، وربما إجراءات أكثر جذرية.

تنطبق الأسئلة الثلاثة في الشكل على كل شيء نقوم به. يتطلب النجاح الإجابة ب "نعم" على الأسئلة الثلاثة كلها، وعندما يكون الجواب هو "لا"، لن يكون هناك أي تحسن دون عمل. يهدف هذا القسم إلى توفير مؤشرات إلى القارئ بخصوص ما هي "الأشياء الصحيحة"، "الطريق الصحيح" و "الجيد بما فيه الكفاية". قد يكون لكل منظمة مجموعات مختلفة من الإجابات على هذه الأسئلة، والتي تعد أمراً متوقعاً، كما أن هناك العديد من الخيارات للاختيار من بينها.

ثانياً: مكونات حاكمية أمن المعلومات

The components of information security governance

يشمل الإطار العام لحاكمية أمن المعلومات العديد من المكونات المترابطة والمتكاملة هي: تحديد الاهداف الاستراتيجية لأمن المعلومات، صياغة الاستراتيجية الأمنية للمنظمة، إعداد سياسات أمن المعلومات، بناء ثقافة المساءلة عن البيانات، وتحديد الادوار والمسؤليات. ويوضح الشكل (3 ـ 2) هذه المكونات.



الشكل (3 ـ 2)

مكونات حاكمية أمن المعلومات

وفيما يأتي نستعرض هذه المكونات.

1- الاهداف الاستراتيجية لأمن المعلومات:

يشير خبراء الأمن إلى أن الأهداف الاستراتيجية لأمن المعلومات والتي يتعين تحقيقها لحماية المعلومات يمكن إختصارها في ما يلي:

أ- الأهداف الاستباقية:

وهي الأهداف التي تسعى حاكمية المعلومات إلى تحقيقها قبل حدوث الاختراق الأمني وتتضمن الأهداف التالية:

- تجنب الخسارة عن طريق حماية الأصول/ الموجودات من التهديدات، من خلال منع التهديدات للأصول/ الموجودات، أو عن طريق إعادة صياغة المتطلبات الأمنية.
- ردع التهديدات من خلال تغيير قيم الافراد ودوافعهم، أو من خلال العقوبات وإزالة أو الحد من أسباب الخسارة.
- الوقاية من الخسارة من خلال وضع الحواجز والتحكم بالوصول.

ب- أهداف رد الفعل:

وهي الأهداف التي تسعى حاكمية المعلومات إلى تحقيقها بعد حدوث الاختراق الأمني وتتضمن الأهداف التالية:

- الكشف عن الحالات الشاذة، والخسائر، والجناة والإعلام الفعال.
- نقل المسؤولية، على سبيل المثال من خلال التأمين.
- التخفيف من حدة الخسارة.
- زيادة العقوبات عن سوء الامن والمكافآت للأمن المثالي.
- تغطية واسترداد الخسارة.
- تصحيح نقاط الضعف.

2- الاستراتيجية الأمنية للمنظمة:

The organization's security strategy

يعد أمن المعلومات في نظر المديرين التنفيذيين والإدارة العليا، وظيفة تدعم الأعمال المنظمية، فهي بلا شك وظيفة مهمة، ولكنها أيضا عنصرا من عناصر التكلفة للمنظمة. ولذلك، تصف استراتيجية أمن المعلومات كيفية التحول من حالة "كما هي as is " إلى حالة "الوجهة الهدف target

destination ". وعند القيام بذلك، تقرر الإدارة العليا كيفية الانفاق الأفضل لأموال المنظمة المحدودة. من هنا وبما أنه من الصعوبة أن تستهدف نفقات أمن المعلومات تقدير المخاطر والنتائج المستقبلية، فإن الاستراتيجية الجيدة تهدف إلى الحد من خطر حدوث شيء سيء حقا، والتي بالتالي سيصبح فائدة افتراضية يتوقع الحصول عليها. ذلك لأنه عند مقارنة المشاريع التي تسهم في تجنب التكاليف غير الملموسة (مثل الأمن) مع مشاريع الاستثمارات التقليدية الموجهة للربح يتعذر الحصول على إجابات سهلة. الاحتياجات من المعلومات لدعم استراتيجية أمن المعلومات تشتمل على:

- توصيات مراجعة الحسابات ذات الصلة وحالة تنفيذها.
- حوادث أمن المعلومات السابقة ونتائجها التشغيلية والمالية.
- مقاييس الأمن مثل مؤشرات الأداء والمخاطر.
- تقييم مدى ونوعية الضوابط الموجودة (على النحو المنصوص عليه من قبل التدقيق الداخلي).
- تحليل أثر الأعمال.
- سجل مخاطر المعلومات، بما في ذلك حالة إجراءات التخفيف/ الحد المخطط لها.
- استخبارات أمن المعلومات ("ما يجري هناك؟").
- تقارير عن حالة الامتثال (التنظيمية والقانونية ومع السياسات الداخلية).

مما سبق يجب أن تتضمن استراتيجية أمن المعلومات في المنظمة وصفا تفصيليا بما فيه الكفاية لأهداف المنظمة، الأولويات، السياسات لتنظيم وتمويل البرنامج.

3- السياسات الأمنية للمنظمة:

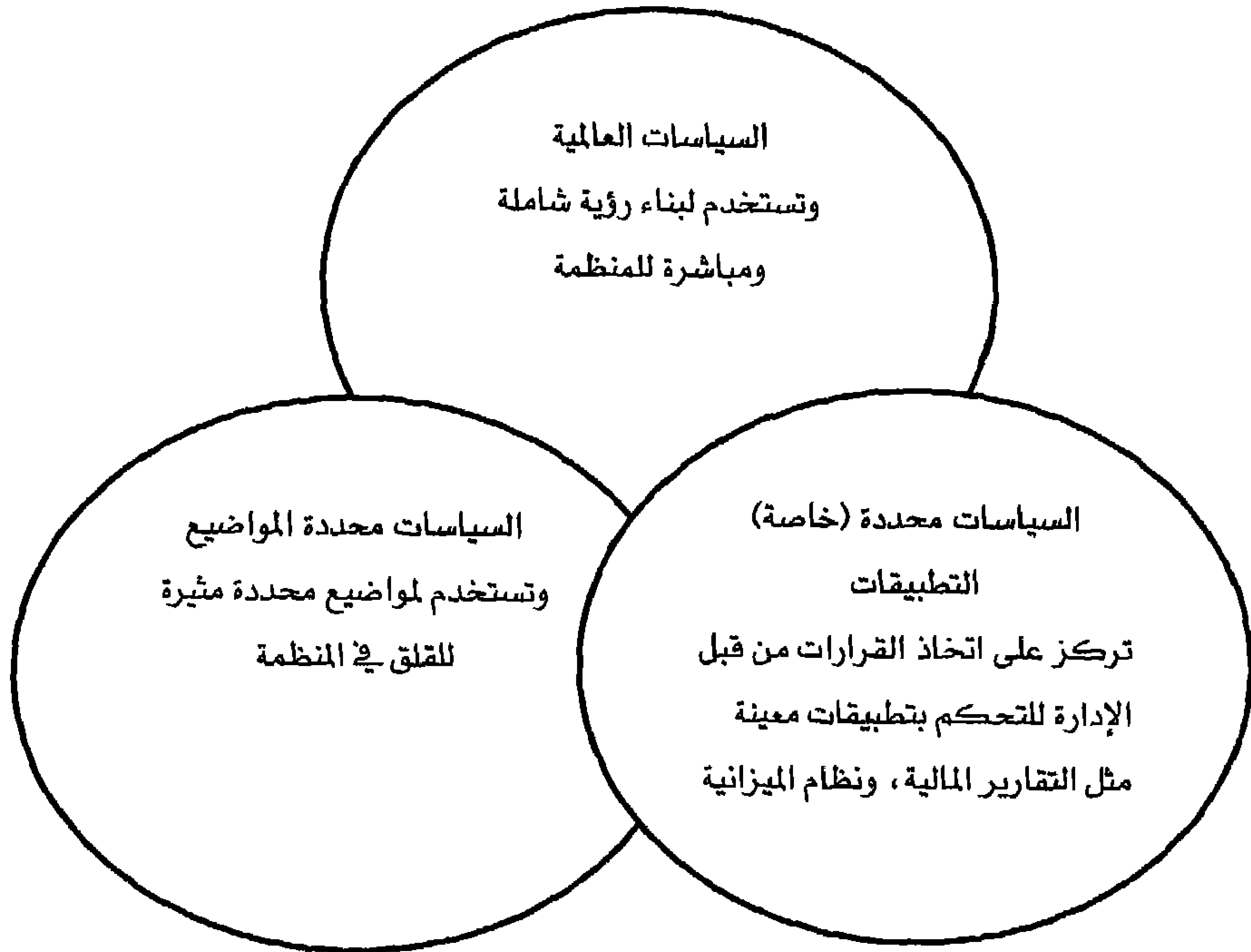
The organization’s security policies

لا يجب أن تقرر السياسة الأمنية التي لا يمكن أو لن تستطيع تنفيذها
Never issue a security policy that you cannot or will not enforce

تعد سياسة أمن المعلومات من العوامل المهمة جداً لضمان توفرعوامل التحكم المناسبة، كما أنها تعد آلية مفيدة لتشكيل سلوكيات الموظفين أو التأثير عليها فيما يتعلق بكيفية إستخدام مصادر نظم المعلومات التنظيمية **(Ifinedo, 2012)**، من هنا تشكل هذه السياسات مجموعة من الوثائق التي تصف المتطلبات والقواعد التي يجب الامتثال لها. ويعرف (النجار، **2011**) سياسة أمن المعلومات على أنها: "مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأه وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها". ويشير **(Peltier, 2004)** إلى ثلاثة أنواع من السياسات التي يمكن استخدامها في أوقات مختلفة في برنامج حاكمية أمن المعلومات وهي كما موضحة في الشكل (3 ـ 3):

- السياسات العالمية: تستخدم هذه لإنشاء رؤية شاملة ومباشرة للمنظمة.
- السياسات محددة المواضيع: تستخدم هذه السياسات لمواضيع محددة مثيرة للقلق في المنظمة.
- السياسات محددة (خاصة) التطبيقات: تركز على إتخاذ القرارات من قبل الإدارة للتحكم بتطبيقات معينة مثل التقارير المالية، ونظام الميزانية.

وتهدف هذه السياسات بغض النظر عن نوعها وآلية تطبيقها إلى تحقيق الآتي: (عرب، **2001**)، (النجار، **2010**)



الشكل (3 ـ 3)

سياسات برنامج حاكمية أمن المعلومات على المستوى العام

- تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسبة والشبكات وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها ومعالجتها وخزنها ونقلها وإعادة استرجاعها.
- تحديد الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر.

- بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك.

في ضوء هذه الاهداف، فإن أي وثيقة أو تقرير سياسة لأمن المعلومات يجب أن يعكس حاجة المنظمة في الجوانب الآتية: (الهادي، 2012)

	طبيعة الحاجة
1	الحاجة لخطة الطوارئ.
2	الحاجة لمساندة حفظ البيانات والمعلومات بفاعلية وكفاءة.
3	الحاجة لتجنب البرمجيات الخبيثة.
4	الحاجة لتوفير إجراءات الرقابة على الوصول لنظم المعلومات ومحتوياتها.
5	الحاجة لاعداد تقرير بالأحداث التي تتعرض لها المنظمة فيما يخص أمن معلوماتها
6	الحاجة لتحديد الإجراءات المطلوب إتخاذها عند حدوث عدم التوافق مع السياسة.

الجدول (3 ـ 1)

الحاجات التي تتضمنها وثيقة سياسة أمن المعلومات

بناءاً عليه ولأجل تحقيق الوضوح والإيجاز في إعداد هذه السياسات، ينبغي أن تغطي كل سياسة مجالاً واحداً. على سبيل المثال، فإن سياسة "كلمة المرور" تغطي القواعد والأنظمة لإنشاء كلمة المرور وصيانتها وتغييرها. إذ يجب أن تتضمن محفظة الشركات على العديد من السياسات، على سبيل المثال لأجل الاستخدام الملائم لموارد المعلومات، إستخدم شبكات

(WiFi) العامة غير المشفرة، قم بتحميل البرمجيات على الأجهزة المستخدمة للوصول إلى بيانات الشركات، وما إلى ذلك.

ولتحقيق النجاح لهذه السياسات، ينبغي مراجعتها والموافقة عليها من قبل أولئك الذين قد يضطرون إلى التعامل مع قضايا عدم الامتثال، وعادة ما تكون وظيفة الموارد البشرية والمستشار القانوني، إلى جانب التشاور مع ممثلي القوى العاملة خطوة جيدة بهذا الاتجاه.

إن إصدار ونشر هذه السياسات يمثل تحدياً، وأسهل طريقة لنشر السياسات تكون في الشبكة الداخلية للشركات والاعتماد على الموظفين للعثور عليها والإحاطة علما بها. فمن غير المعقول أن نتوقع أن يكون مثل هذا النهج فعالاً. والمثل الذي يقول "يمكنك أن تأخذ الحصان إلى الماء ولكنك لا يمكنك أن تجعله يشرب" يعبر عن كل شيء. وعلى الطرف الآخر، هناك طرق لضمان أن يتلقى كل موظف نسخة من هذه السياسة، يقر من خلالها بالاستلام ويوقع على وثيقة تفيد نيته للامتثال. ويودع هذا المستند في سجل الموارد البشرية لكل فرد. هذا النهج معقد جدا. حيث يجب التأكيد على أن أمن المعلومات ليس أمراً فنياً فقط يمكن تصحيحه والتغلب عليه بإعتماد جدران النار (Firewall)، بل يمثل أيضاً عملاً إدارياً يجب على القوى العاملة بالمنظمة والأطراف الأخرى المتعاونة معها الإعتراف بإستلام تقرير سياسة أمن المعلومات والتعهد بتطبيق ما جاء به من مبادئ ومعايير وقبول مقاييس صارمة في حالة عدم الإلتزام بذلك (الهادي، **2012**). باختصار، ينبغي أن يعكس النهج الذي يتم اختياره أهمية أمن المعلومات للمنظمة والثقافة السائدة فيها.

4- ثقافة المساءلة عن البيانات:

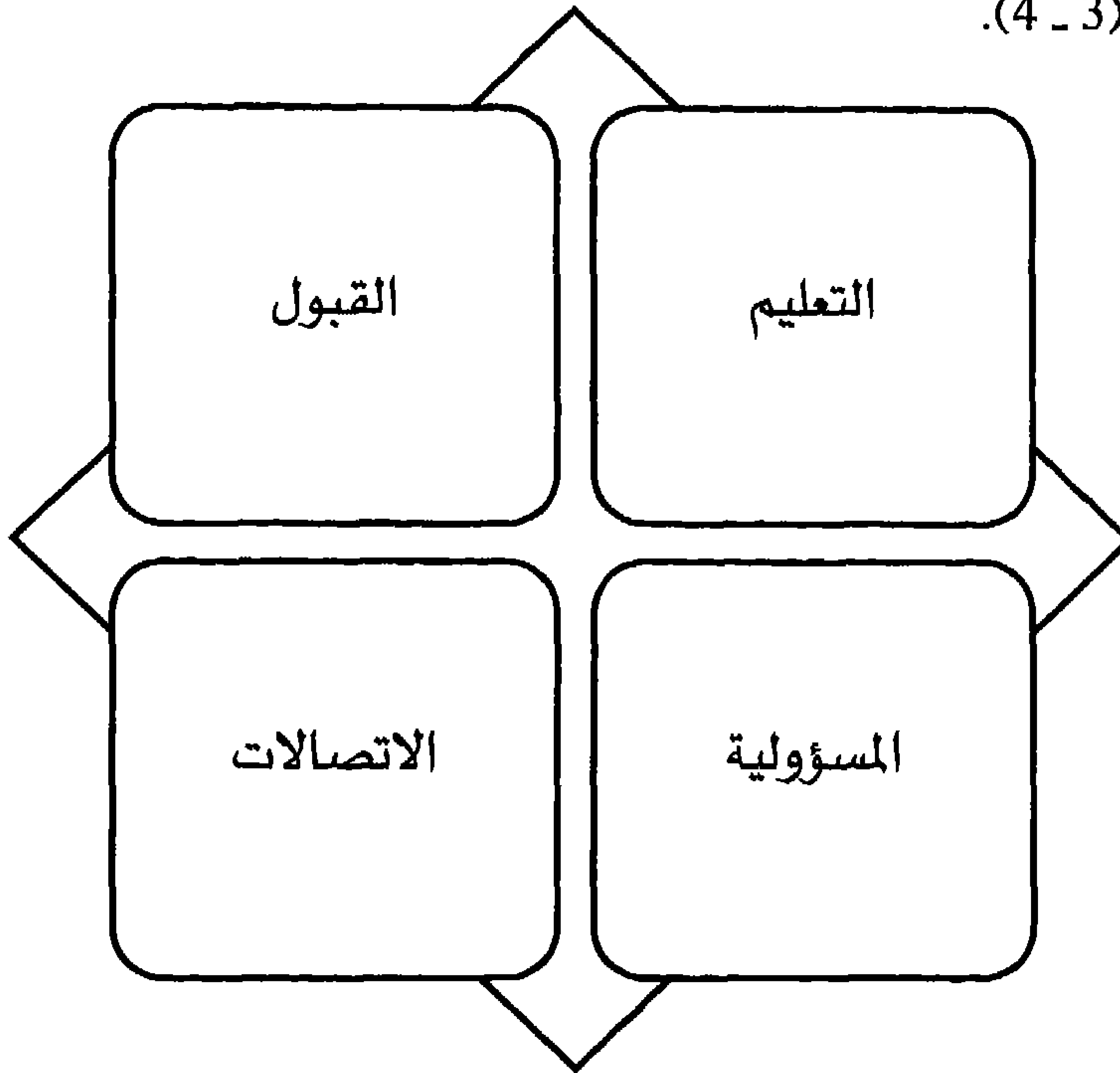
The Culture of Data Accountability

المدخل لهذا الموضوع هو السؤال: ماذا تعني ثقافة المساءلة عن البيانات وكيف يمكن بناء هذه الثقافة ؟ للاجابة عن هذا التساؤل نشير إلى المساءلة بشكل عام والتي تعني الرغبة في أن تكون مسؤولاً عن شيء ما، وفي الاستخدام اليومي، تعني المسؤولية التزاما من قبل جهة معينة تجاه شيئ ما، أي أن تفعل هذه الجهة ذلك الشئ أو أن ترى أن الشئ يحصل فعلياً. من هنا فان تكريس ثقافة المساءلة عن البيانات يستلزم أن تشير "البيانات" ـ كجزء من مصطلح "حاكمية أمن المعلومات" ـ ضمنيا إلى حق البيانات (data, right)، ذلك لأنه في الواقع، فإن الحاكمية الفاعلة لأمن المعلومات ليست حول نظم المعلومات بحد ذاتها على الإطلاق. بدلا من ذلك، انها حول تغيير كيف يمكن أن تكون نظرة المنظمة والعاملين فيها إلى البيانات الخاصة بها. فبدون البيانات، لا توجد حاكمية لأمن المعلومات، ولكن الحاكمية الفاعلة تذهب إلى أبعد من البت والبايت. انها ترتبط بالتحول الثقافي بعيدا عن التفكير في البيانات كسلعة نحو التفكير بالبيانات بوصفها واحدة من أصول(موارد) المنظمة الأكثر قيمة، وخلق العقلية المنظمية للمساءلة. ويمكن تعريف ثقافة المساءلة عن البيانات على أنها: الحالة التي يحرص فيها كل فرد في المنظمة على تحمل واجب المساعدة في تنفيذ برنامج حاكمية أمن المعلومات، وأن يكون مسؤولاً عن نجاحها أو فشلها، وفقا للدور الذي يضطلع به.

في ضوء هذا التعريف، ترتكز ثقافة المساءلة عن البيانات على أربع ركائز (أعمدة) أساسية هي (**Griffin, 2011**):

- التعليم (Education).
- القبول (in ـ Buy).
- المسؤولية (Responsibility).
- الاتصال (Communication).

وفيما يأتي فكرة موجزة عن هذه الركائز الأربعة الموضحة في الشكل (3 ـ 4).



الشكل (3 ـ 4)

الركائز الأربعة لثقافة المساءلة عن البيانات

أ- التعليم:

ينطوي على جعل الأفراد العاملين في المنظمة على بينة من برنامج حاكمية أمن المعلومات وخلق مستوى أعمق من الفهم لكيفية الحصول على

البيانات ومعالجتها وإستخدام المعلومات، إلى جانب فهم العمليات المنظمية التي تستخدم البيانات وكيف تؤثر تلك البيانات في العمليات الأخرى. في الأساس، من أجل تفعيل دور حاكمية أمن المعلومات، يجب أن يعلم الأفراد كيفية تحقيق البرنامج الفائدة لهم على وجه التحديد في وظائفهم. فمن السهل إثبات كيفية مساعدة جودة البيانات والسياسات والإجراءات الموحدة للبيانات للمنظمة في الحصول على منافع معينة، لكنه من الأهمية أيضاً الإثبات للعاملين في مجال المعرفة كيف أن حاكمية أمن المعلومات (أو وجود قصور فيها) سوف تؤثر عليهم وكيف يمكن أن تؤثر على الأفراد الآخرين في المنظمة كذلك. على سبيل المثال، إذا كان أثناء تنفيذ عملية منظمية معينة، الإدارة المالية تنتج وتستخدم مجموعة بيانات معينة يمكن أن تستخدم لاحقاً من قبل إدارة التسويق في عملياتها، فانه يجب على العاملين في الادارة المالية أن يدركوا كيف أن البيانات وجودتها ستؤثر على عملية التسويق. ومن الضروري إعلام الأفراد حول الطريقة التي يمكن أن تستفيد بها من وجود سياسات وإجراءات حاكمية أمن المعلومات التي تحتم توحيد البيانات واتساقها. ولأجل تعزيز عنصر التعليم تقتضي الضرورة إنشاء مجلس يسمى مجلس " حاكمية أمن المعلومات " في المنظمات يتحمل المسؤولية عن الجهود التعليمية، كما ينبغي أن تكون هناك رسالة واضحة ومتسقة لتوضيح فوائد برنامج حاكمية أمن المعلومات والتواصل الفعال. وينبغي أن تستهدف تلك الرسالة الدور بحيث يمكن لأي فرد في المنظمة أن يفهم ما هو البرنامج وكيف يستفيد منه شخصياً.

ب- القبول/الإيمان:

حالما يتوصل العاملون في مجال المعرفة إلى فهم حقيقي لغرض برنامج حاكمية أمن المعلومات وفائدته، يتم وضع الأساس للدعامة الثانية لثقافة المساءلة عن البيانات، والتي هي القبول/الإيمان وذلك عندما يقبل الأفراد العاملون الفكرة، ويصبحوا مقتنعين بشدة بأن هذه الفكرة مفيدة، وأنه هو ببساطة الشيء الصحيح الذي ينبغي القيام به. ولتحقيق القبول - وخاصة بين العاملين في مجال المعرفة - نجد من الضروري جعل الأفراد العاملين جزءاً لا يتجزأ من الحل. المحرك الاساسي لعملية القبول يتمثل في مبدأ جوهري هو أن الافراد العاملين الذين ينفذون العمليات المنظمية التي تنتج وتستخدم البيانات هم أصحاب البيانات حقا وهم المشرفين عليها وهم الذين يجب منحهم حق ملكية البيانات، وأن نتعهد لهم بتنفيذ سياسات وإجراءات حاكمية أمن المعلومات. بتعبير آخر يستلزم تحقيق نتائج إيجابية من تطبيق برنامج حاكمية أمن المعلومات في كثير من الأحيان وحشد المساندة من العاملين في مجال المعرفة من أجل تحسين سياسات وإجراءات حاكمية أمن المعلومات التي تحتاج إلى التغيير والتبديل. ولا يتوقف الامر عند حاجة عمال المعرفة إلى الاعتقاد في حاكمية أمن المعلومات، ولكن برنامج حاكمية أمن المعلومات يتطلب حصول قناعة الادارة التنفيذية أيضاً، فبدون الرعاية القوية من قبل الادارة التنفيذية، قد لا يقترب البرنامج أبدا بشكل كامل عن ارض الواقع. الرعاية القوية من قبل الادارة التنفيذية ضرورية لتكون بمثابة حافز لبرنامج حاكمية أمن المعلومات، ولكنها ضرورية أيضا لضمان استمرارية نجاح البرنامج - خاصة وأنها ترتبط بتخصيص الموارد اللازمة لتحريك الجهود

للمضي قدما، إلى جانب تحديد الأولويات الاستراتيجية الخاصة بتنظيم وتوجيه إدارة البيانات كمورد حيوي للمشاريع الهامة في المنظمة.

ج- المسؤولية:

الركيزة الثالثة لثقافة المساءلة عن البيانات هي المسؤولية. إذ أنها لا تعد كافية لمجلس حاكمية أمن المعلومات والعاملين في مجال المعرفة والاعتقاد ببساطة في نجاح حاكمية أمن المعلومات. بل يجب على الجميع في المنظمة تحمل كامل المسؤولية عن كل ما يتعلق بالبرنامج. بعض الافراد العاملين حريصون على قبول وتحمل المسؤولية عن شيء ما يرونه مفيدا من أجل أنفسهم والآخرين (عندما تتطابق مع مصالحهم الشخصية)، وبالمقابل، فإن كثير منهم ليسوا كذلك. من هنا وبهدف غرس أخلاقيات المسؤولية، نجد من الضروري تحفيز الافراد العاملين وحثهم على المشاركة الفاعلة مع التحديد بشكل رسمي للأدوار والمهام. ويبرز دور مجلس" حاكمية أمن المعلومات " مجددا إلى الواجهة مرة أخرى. وفي بداية البرنامج، ينبغي أن تكون هناك محاولة وبشكل رسمي لتحديد وتعيين أدوار ومسؤوليات حاكمية أمن المعلومات، كما ينبغي تحديد ملكية البيانات (Data ownership)، والإشراف عليها (stewardship) وتوضيح السياسات والإجراءات الخاصة بها في جميع أنحاء المنظمة. هذا هو الوقت المناسب لوضع مقاييس واقعية لقياس فاعلية برنامج حاكمية أمن المعلومات وتثبيت آلية الحوافز لمكافأة أولئك الذين يحققون مستويات الاداء المستهدفة أو يتجاوزونها.

د- الاتصالات:

الدعامة الرابعة لثقافة المساءلة عن البيانات هي الاتصالات. قد يمكن للمنظمة ضمان مساندة الادارة التنفيذية واقناع العاملين في مجال المعرفة لأهمية

البرنامج وإضفاء الطابع الرسمي على الأدوار والمسؤوليات، ولكن برنامج حاكمية أمن المعلومات يمكن أن يفشل بسبب ضعف الاتصالات. الاتصالات، في الواقع، تعد الأساس للركائز الثلاث الأخرى اللازمة لبناء ثقافة المساءلة عن البيانات. منذ البداية وللإبلاغ عن برنامج حاكمية أمن المعلومات تعد الاتصالات أداة حاسمة لبناء الوعي بأهمية هذا البرنامج. الاتصالات أمر حيوي لتحقيق القناعة لدى العاملين في المنظمة ككل. ويمكن أن ينعكس الاستيعاب الحقيقي لقيمة حاكمية أمن المعلومات بطرق كثيرة، أحدها هو الاتصالات الرسمية عن كيفية أولئك الذين يقومون برعاية برنامج حاكمية أمن المعلومات من قبل المنظمة. المدير التنفيذي للمعلومات يمكن أن يكون رائداً في هذه المبادرة وفي كسب ثقة العاملين في مجال المعرفة في مختلف مستويات المنظمة. أخيرا، يمكن للاتصالات الواضحة سد الفجوة وتحقيق المواءمة بين الأدوار والمسؤوليات المحددة رسميا واستيعاب تلك الأدوار والمسؤوليات من قبل العاملين في مجال المعرفة. وإحدى الطرق لتعزيز هذا التوافق هي من خلال رسم خارطة الطريق لحاكمية أمن المعلومات. على مستوى عال، بحيث تسهم هذه الخارطة في توصيل ثلاثة أشياء مهمة هي:

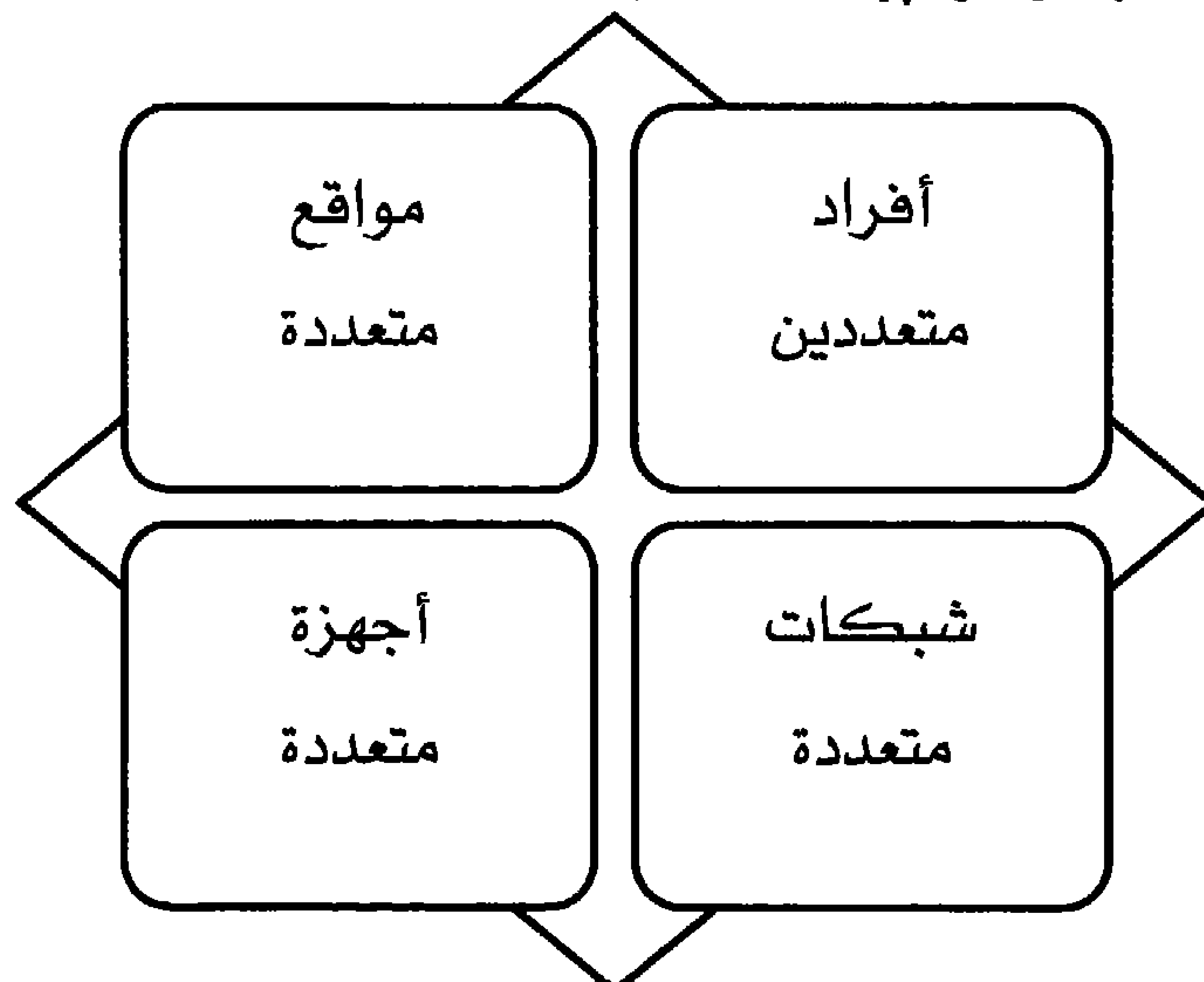
- الأدوار والمسؤوليات والمتطلبات اللازمة لحاكمية أمن المعلومات في جميع أنحاء المنظمة.
- خطة للمساعدة على تلبية هذه المتطلبات وإدامة كفاءة حاكمية أمن المعلومات للمضي قدما.
- مقاييس للمساعدة في قياس التقدم المتحقق لأداء برنامج حاكمية أمن المعلومات.

5- مسؤولية أمن المعلومات على مستوى المنظمة:

Accountabilities for information security across the organization

لقد أوجد التقدم التقني البيئة التي تسمح بالوصول إلى مصادر المعلومات ومن ثم السمات الأساسية لهذه البيئة، كما هو موضح في الشكل (3 ـ 5):

- لأفراد متعددين (سواء كانوا داخل المنظمة أم لا).
- من مواقع متعددة (المكاتب والمنازل، أثناء التحرك).
- استخدام شبكات متعددة (الشركات، والإنترنت، والمنزل، لاسلكي تجاري، الهاتف).
- مع أجهزة متعددة (أجهزة الحاسبات للشركات والمنزل، والأقراص، والهواتف الذكية).



الشكل (3 ـ 5)

السمات الأساسية لبيئة الوصول إلى مصادر المعلومات

في ظل هذه البيئة، فإن العديد من العناصر ليست تحت سيطرة الشركات وليس من الممكن بالتالي أن نتوقع وجود شخص معين ليكون مسؤولاً بالكامل عن أمن أصول/موجودات المعلومات. وينبغي أن يكون الجميع على استعداد لتقديم مساهمة فعالة. من هنا يجب رفع شعار" الحفاظ على الأمن هو مهمة الجميع Maintaining security is everybody's job ". إلا أن تجسيد هذا الشعار ليس بالأمر البسيط، ذلك لإنه لا يمكن تطبيق برنامج حاكمية أمن المعلومات بالقوة، ولكن. يجب أن يكون كل فرد في المنظمة من أعلى الهرم التنظيمي إلى قاعدته على بينة من أهميته. يجب عليهم الاقتناع بتلك الأهمية، ويجب عليهم تحمل المسؤولية وفقا للدور الذي يسهم به لاستمرار نجاح جهود حاكمية أمن المعلومات. وبعبارة أخرى، يجب على المنظمة بأكملها أن تكون على استعداد لتكون مسؤولة عن نجاح حاكمية أمن المعلومات. إن تحقيق مستوى مرض من أمن المعلومات يتطلب أشياء كثيرة ينبغي القيام بها، وهذه الأمور تتطلب القيادة الناجحة لجهود أمن المعلومات إذا ما أريد لها أن تنجز العمل جيداً بما فيه الكفاية. لتوضيح هذا، نأخذ قياسا على الأوركسترا وقائدها: يوفر القائد القيادة من خلال جعلها واضحة إلى الموسيقيين، كل فرد هو خبير ومدير على آلته الموسيقية، ومسؤول عن أدائه كجزء من مجموعة. لا يحتاج القائد أن يكون قادراً على العزف على كل أداة في الاوركسترا ولكن يجب أن يكسب مصداقية وإحترام العازفين. القائد الرائع يمكنه الحصول على أداء جيد من أوركسترا متوسطة. عندما لا يكون القائد جيداً ويقوم بقيادة أوركسترا جيدة، فإن أعضائها عادةً ما

يقـدمون أداء جيـداً مـن خـلال تجاهـل هـذا القائـد. عنـدما يكـون مـستوى الأوركـسترا وقائـدها متوسـط، فـسوف تكـون النتيجـة في أحـسن الأحـوال متوسطة. فكما هو الحال بالنسبة لنموذج سمفونيـة الأوركـسترا أعـلاه، فإن الأداء الجيد يتطلب من كل عضو في الفرقة أن يبذل قصارى جهده من أجل ذلك. في مجال أمن المعلومات، يتطلب ذلك فهماً واضحاً للأدوار والمسؤوليات، ومعرفـة العمليـات المنظميـة ذات الـصلة ودور نظـم المعلومـات والبيانـات في دعمها، والخبرة، والدافع والالتزام.

وأسهل طريقة لمعرفة أن المهام الرئيسية لم يتم تنفيذها هـو عدم وضـوح مـن يكـون مـسؤولاً عـن شـئ مـا. في المنظمـات الكـبيرة، حيـث أن الحجـم والتعقيد يتطلبان إجـراءات رسميـة، تـدرج المساءلة أيضا في توصيـف الوظـائف لتجنـب حالـة "لا توجـد في وصـف وظـيفتي" كمتلازمـة موجـودة خاصـة عنـد التعامل مع حالة فض الاشتباك بين الموظفين. بالإضافة إلى ذلك هنـاك أدوار يجـب تنـسيبها إلى الافـراد خـارج وظيفـة تكنولوجيـا المعلومـات (خارجيـة أو داخلية) لتحديد احتياجات حساب الوصول، النظام والبيانات، والموافقة على الاستثناءات، وما إلى ذلك، كما هو موضح أدناه.

أ- تخصيص الموارد، البشرية والمالية:

Resource allocation, human and financial

ربما تعد هـذه المهمـة الأكثـر أهمية في إطـار حاكمية أمـن المعلومـات، حيث تتطلب صنع قرارات متسقة مع تقييم كل من الجوانب الاتية:

- الأداء الحالي لأمن المعلومات، أي هل هو جيد بما فيه الكفاية؟

- المعرفة والخبرة والشهادات لأولئك الذين يتحملون المسؤولية عن أمن المعلومات.
- مدى ونوعية الضوابط القائمة (التدقيق الداخلي لا نعتبرها كافية؟)
- هل يشكل أمن المعلومات جزءاً من تكلفة ممارسة الأعمال المنظمية أو استثمارات المنظمة؟
- كيف يجب تبرير هذه النفقات.
- ملاءمة الأداء الحالي والضوابط الحالية.
- الحاجة المستقبلية من الموارد البشرية لدعم أنشطة أمن المعلومات.

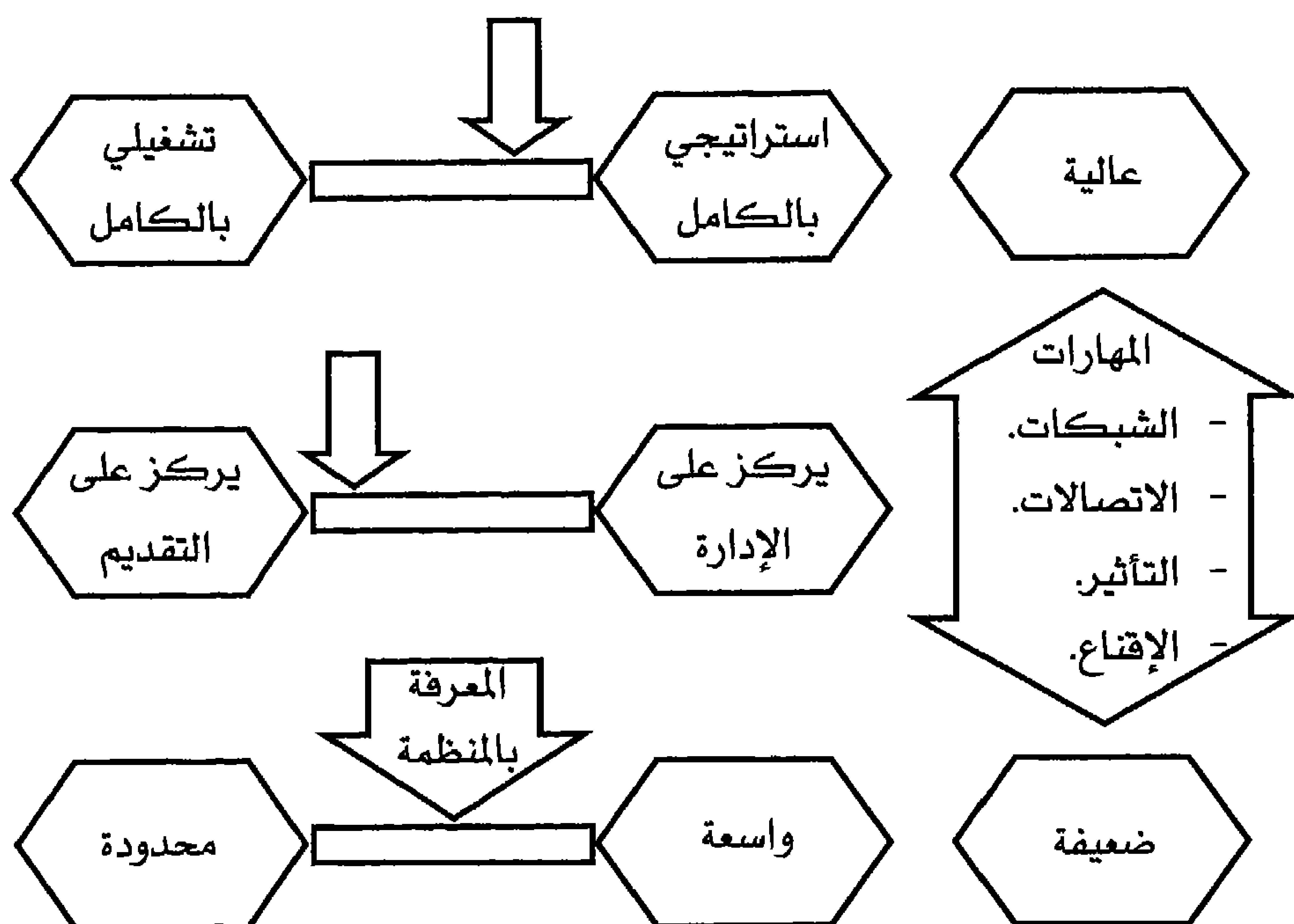
فإن نوعية هذه القرارات هي التي تحدد ما إذا كانت استراتيجية أمن المعلومات ستنجح أو ستفشل.

ب- وصف دور كبير ضباط أمن المعلومات:

Chief Information Security Officer (CISO)

في البداية... (20 إلى 25 سنة ماضية) كانت وظيفة أمن المعلومات مدمجة مع وظيفة تكنولوجيا المعلومات وينظر إليها على أنها دور تقني. لقد تغير الزمن، وبالتالي فإن الأدوار المحتملة متعددة للمهنيين في أمن المعلومات.

الأسهم في الشكل (3 ــ 6) يمكن وضعها في أي مكان على طول الخط الفاصل بين النقاط واصفا دور كبير موظفي أمن المعلومات. الإدارة العليا (بما في ذلك كبير موظفي المعلومات) تحتاج إلى تحديد أي الخيارات هي الأنسب لمنظمتهم.



الشكل (3 ـ 6)

إختيار الدور الأنسب لكبير موظفي أمن المعلومات

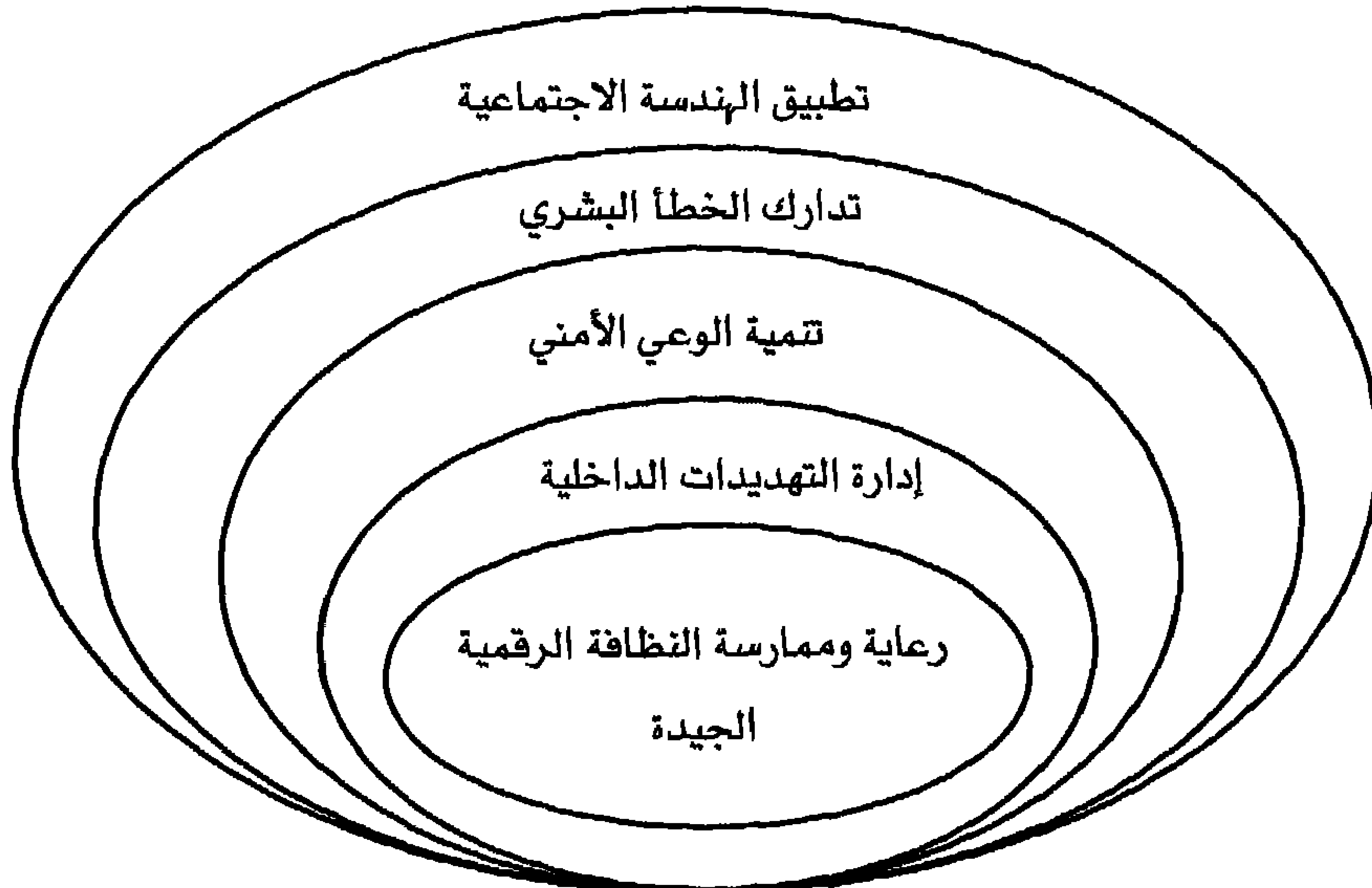
والسؤال الأول الذي يطرح هنا هو هل هذا الدور تشغيلي أو استراتيجي (Is the role operational or strategic)؟. فالدور الاستراتيجي يتطلب التفاعل مع العديد من المديرين، بما في ذلك الرئيس التنفيذي للمعلومات، كبير ضباط الأمن، رئيس إدارة المخاطر، التدقيق الداخلي، المستشار القانوني العام والعديد من وحدات الأعمال ـ وكذلك مع الإدارة التنفيذية ومجلس الإدارة. وهذا يتطلب من (CISO) امتلاك معرفة جيدة عن الأعمال ومهارات البرمجة: الاتصالات، والعلاقات الشخصية، والمفاوضات والأخلاق. وبالإضافة إلى ذلك، فإن المظهر والمصداقية ضرورية.

والسؤال الثاني الذي يجب الاجابة عليه هو هل يتم التركيز في إطار هذا الدورعلى تقديم الخدمات أو على الإدارة Focus on delivery or on

(management)؟. إذ يوصف دور تقديم الخدمات بأنه وظيفة فنية تتطلب معرفة بالمنتجات والإجراءات، والأفراد الذي يشغلون هذا الدور غالبا ما يكونوا غير مرئيين للمنظمة وتكون الحاجة إلى المهارات الناعمة هي أقل أهمية لشغل هذا الدور. أما الإدارة التشغيلية فإنها تتطلب (CISO) لإدارة أنشطة وأداء العديد من الأخصائيين التقنيين ويكون لديهم معرفة جيدة في التخصصات ذات الصلة مثل إدارة المخاطر، واستمرارية الأعمال، وحماية الملكية الفكرية، وتسرب البيانات وقضايا السلامة، والامتثال التنظيمي، والخصوصية، والطب الشرعي والتحقيقات، إلخ

ج- **دور المدراء الآخرين** Your role as a manager:

قد لا تظهر في الوصف الوظيفي الخاص بكل مدير مسؤولية إدارة أمن المعلومات، ولكن الأمن هو حقا "وظيفة الجميع". عليه يتعين على المديرين القيام بالأدوار الخمسة الآتية، كما هي موضحة في الشكل (3 ـ 7):



الشكل (3 ـ 7)

دور المدراء الآخرين في حماية أمن المعلومات

- تنمية الوعي الأمني **Develop security awareness**:

كلما يقول أي فرد: "لم أكن أعرف"، هذا يخلق ثغرة وبالتالي يمثل خطرا على المنظمة. وينبغي للأفراد في فريقك أن يدركوا ضرورة الحفاظ على الأمن وأيضا معرفة لماذا تعد سياسات أمن المعلومات في المنظمة والامتثال لها شيئاً مهماً. حيث يتضمن بعض عقود العمل شروطا محددة لأمن المعلومات مثل عدم الإفصاح عن المعلومات السرية، الحساسة أوغيرها من التصنيفات. وقد تتطلب الدوائر الحكومية توقيع شيء يعادل قانون الأسرار الرسمية. كما قد يتم تطبيق معايير مماثلة لمعلومات العملاء، بدءا من الاسم والعنوان ومعلومات الاتصال وصولاً إلى حالة العملاء، على سبيل المثال تصنيف الائتمان والأرصدة لدى البنوك وغيرها قد تكون خاضعة للتشريعات الوطنية مثل حماية البيانات والخصوصية. وكان الكشف عن الآلاف من التبادلات الدبلوماسية من قبل أحد أفراد الخدمة من الجيش الأمريكي، في اطار ما سميت "تسريبات ويكي Wiki leaks " في عام 2010، أحد الحالات لقيام فرد يمتلك الصلاحية للوصول إلى المعلومات بإساءة استخدام هذا الامتياز وقام بتسريب المعلومات لأسباب غير معروفة، بغض النظر عن العواقب التي تنتظر المنظمة والفرد.

- إدارة التهديدات الداخلية **Manage internal threats**:

وتعد هذه جزءاً من مسؤوليات كل مدير ويشمل ذلك تحديد ما يلي:

- عدم التقيد بالسياسات.
- موظفين فاقدين للحفز والتحرر.
- جميع أشكال التخريب، فقدان المعدات أو البيانات، وسرقة الملكية الفكرية والإفصاحات الأخرى غير مصرح بها، والاحتيال، وما إلى ذلك.

وينبغي استشارة دائرة الموارد البشرية، المستشار القانوني وشركات الأمن بشأن هذه المسائل وتعد نصائحهم بشأن التحقيقات أمراً ضرورياً قبل اتخاذ أي إجراء.

- رعاية وممارسة النظافة الرقمية الجيدة:

Sponsor and practice good digital hygiene

كانت عدوى المستشفيات منتشرة في القرن (19) وحتى أوائل القرن (20). النظافة الجيدة والمضادات الحيوية قضت عليها، ولحد الآن نحتاج إلى تعزيز النظافة مرة أخرى بسبب العواقب غير المقصودة مثل ظهور البكتيريا المقاومة للمضادات الحيوية. وفيما يلي نستعرض ممارسات النظافة الجيدة في مجال أمن المعلومات:

- حماية المعدات والبيانات من الضياع أو السرقة والإبلاغ الفوري كلما يحدث هذا؛
- الحفاظ على البرنامج المحدث (وخاصة المعدات المملوكة للمستخدم النهائي).
- تطبيق كلمات المرور مصممة بشكل جيد ويتعذر تخمينها، و الأفضل، استخدام أسلوب التحقق (factor _ two) وعدم مشاركة كلمات السر مع الآخرين بتاتاً.
- تركيب وصيانة أدوات محدثة لمنع الوصول غير المصرح به (مثل جدار الحماية) والمانع أو إزالة البرامج الضارة (مثل مكافحة الفيروسات).
- القيام بالرعاية المناسبة بعدم الكشف عن المعلومات الحساسة من خلال وسائل الاعلام الاجتماعية (مثل الفيسبوك وتويتر و Linkedin).

- استخدام التشفير لحماية البيانات الحساسة إذا كان هذا يتماشى مع السياسات الأمنية للمنظمة.
- عمل نسخ من المعلومات (النسخ الاحتياطي) والحفاظ عليها بطريقة آمنة (مشفرة، وخزانات آمنة، ...الخ).

- تدارك الخطأ البشري **Human error**:

الكمال المطلق لله سبحانه وتعالى فلا يوجد شخص كامل، والانشطة غير المقصودة قد تؤثر في أمن المعلومات. إنجاز العمل في مهلة ضيقة، الالهاء، والافتقار إلى التركيز نظرا لتعدد المهام، والانقطاع، والشعور بالإعياء، وما إلى ذلك، كلها تقود إلى حدوث الخطأ البشري. عدم الإلمام بالإجراءات و/ أو الأنظمة فضلا عن الاعتماد على الموظفين المؤقتين يمكن أن يؤدي أيضا إلى الخطأ البشري.

هناك ضوابط للحد من إمكانية حدوث الخطأ البشري. لعل من أهمها مبدأ الفصل بين المهام وهو الأسلوب الذي شاع تطبيقه في أغلب المنظمات، حتى الاتجاه لما يصطلح عليها "المؤسسة المتكئة" والتي اسهمت في خفض أعداد الموظفين لدرجة أن المسؤولية وضعت أكثر وأكثر على الأفراد دون القيام بالتحقق السليم عن دقة وملاءمة أعمالهم.

- تطبيق الهندسة الاجتماعية **Social engineering**:

قرصنة الإنسان ". هي جزء لا يتجزأ من سمة الخداع والتلاعب في الطبيعة البشرية والممارسين الجيدين لا يحتاجون المهارات التقنية لكسر حواجز حماية أصول/ موجودات المعلومات ــ أنهم ببساطة يسألون عن المعلومات أو العناصر اللازمة للوصول إليها. إذ كشفت البحوث التي أجريت

في المملكة المتحدة في السنوات الأخيرة أن العديد من الاشخاص لديهم الاستعداد للكشف عن "معرف" وصولهم وكلمة المرور إلى الحاسبات وملفات المعلومات في مقابل قطعة من الشوكولاته.

ثالثاً: مبادئ حاكمية أمن المعلومات

يمكن أيضا الاقتراب أكثر من مفهوم أمن المعلومات من زاوية تحديد مبادئ حاكمية أمن المعلومات. والغرض من هذه المبادئ هو توفير بعض الأفكار حول الكيفية التي يمكن بها أن تعالج المشاكل العملية لأمن المعلومات في الأنشطة التي تهدف إلى تحقيق غايات أمن المعلومات، والتي تم توضيحها في الفصل السابق. مبادئ أمن المعلومات تصف، على المستوى العام، بعض صفات نشاط أمن المعلومات. وهذه المبادئ يمكن توضيحها باختصارعلى النحو الموضح في الجدول الآتي:

	المبادئ	الوصف
1	المساءلة	يجب توضيح المسؤوليات والمساءلة لكل الأطراف المعنية بأمن نظم المعلومات من المالك، المجهز و مستخدمي نظم المعلومات وغيرها.
2	الوعي	يجب على الأطراف المعنية أن تكون قادرة على اكتساب المعرفة المناسبة، وتكون على علم بوجود التدابير والممارسات و الإجراءات الخاصة بأمن نظم المعلومات ومداها.
3	الأخلاقيات	يجب احترام مصالح الحق والشرعية.

4	التخصصات المتعددة	ينبغي للتدابير والممارسات والإجراءات الخاصة بأمن نظم المعلومات أن تأخذ في الاعتبار جميع وجهات النظر ذات الصلة.
5	التناسب	ينبغي أن تكون مستويات الأمن، وتكاليفه، والممارسات والتدابير والإجراءات مناسبة ومتناسبة مع قيمة ودرجة الاعتماد على نظم المعلومات و مع شدة، واحتمالية ومدى الضرر المتوقع.
6	التكامل	التنسيق والتكامل بين تدابير وممارسات و إجراءات أمن نظم المعلومات.
7	التوقيت المناسب	اشتراط التنسيق في الوقت المناسب بين الجهات العامة والخاصة فيما يتعلق بالوقاية و التصدي لانتهاكات أمن نظم المعلومات.
8	إعادة التقييم	ينبغي إعادة تقييم الأمن بصفة دورية، طالما أن نظم المعلومات ومتطلبات أمنها تختلف مع مرور الوقت.
9	الديمقراطية	ينبغي أن يكون أمن نظم المعلومات متوافقاً مع الاستخدام المشروع ومع تدفق البيانات والمعلومات في مجتمع ديمقراطي.

الجدول (3 ـ 2)

مبادئ حاكمية أمن المعلومات

مما سبق ولاجل التطبيق السليم للمبادئ المذكورة في الجدول السابق فإن الضرورة تقتضي وضع الشروط المناسبة، وفيما يأتي الجدول(3 ـ 3) الذي يوضح أهم هذه الشروط:

1	تناغم المعايير التقنية والأساليب والممارسات.
2	تعزيز الخبرات وأفضل الممارسات.
3	صياغة العقود وصحتها والوثائق الأخرى التي تم إنشاؤها وتنفيذها في نظم المعلومات أو من خلالها.
4	تحديد المخاطر والمسؤولية عن الفشل في أمن نظم المعلومات.
5	العقوبات الإدارية أو غيرها عند إساءة استخدام نظم المعلومات.
6	الولاية القضائية للمحاكم.
7	المساعدة المتبادلة وتسليم المجرمين وغيرها من أشكال التعاون الدولي في الأمور المتعلقة بأمن نظم المعلومات.
8	وسائل للحصول على الأدلة في مجال نظم المعلومات ودرجة قبول هذه الأدلة في الإجراءات القانونية والإدارية.

الجدول (3 ـ 3)

أهم شروط نجاح تطبيق مبادئ حاكمية أمن المعلومات

رابعاً: قواعد السلوك/ المعايير لأمن المعلومات

حتى وإن كانت هناك قواعد/ معايير صريحة وواضحة على نحو متزايد بشأن أمن المعلومات في إطار كل منظمة من المنظمات فإنه يجري جانب هام من الضبط والأحكام عن طريق بعض المؤسسات القانونية الأخرى. هذا قد يؤدي إلى افتراض أن أمن المعلومات لا يتم ضبطه بما فيه الكفاية

داخل المنظمات وبالتالي لا يمنع من التعرف على قواعد السلوك/ المعايير ذات الصلة. وبناءاً عليه فإن المحامين الممارسين والمشرعين ومصممي نظم المعلومات والمديرين بحاجة إلى أن يكونوا قادرين على التعرف على قواعد السلوك/ المعايير ذات الصلة بأمن المعلومات. على سبيل المثال تعد معايير تحديد الهوية الأساسية وظيفة قاعدة السلوك القانونية فيما يتعلق بحماية السرية والتمامية وتوافر (إتاحية) المعلومات ونظم المعلومات. وبهذا الخصوص يمكن التمييز بين مالا يقل عن عشرة مجموعات أساسية من قواعد السلوك/ المعايير لأمن المعلومات، كما هي موضحة في الجدول التالي:

1	قواعد السلوك الخاصة بوضع الشخص تحت الالزام لتوفير أمن المعلومات.
2	قواعد السلوك، والتي تتطلب بشكل غير مباشر أن أمن المعلومات يتم توفيره لأجل.
3	قواعد السلوك التي تحكم مهام و هيكل المنظمات الذي تتمثل مهمته في تعزيز و توفير أمن المعلومات.
4	قواعد السلوك الخاصة بمعاقبة الأفعال الضارة للمعلومات أو نظم المعلومات.
5	قواعد السلوك التي تعزز و تؤمن توافر المعلومات والمحافظة عليها.
6	قواعد السلوك التي تضبط تقييم المخاطر ومدى قبول الأدلة الإلكترونية.
7	المعايير المتعلقة بمنع الجريمة و الأمن الداخلي للدولة.

8	المعايير المتعلقة بالوقاية من التهديدات ضد أمن الدولة الخارجي و حرب المعلومات بالمعنى الأوسع.
9	المعايير التي تنظم خدمات أمن المعلومات والمنتجات.
10	المعايير التي تنظم مستوى أمن المعلومات لتكنولوجيا المعلومات والاتصالات.

الجدول (3 ـ 4)

قواعد السلوك/ المعايير لأمن المعلومات

لقد تم بناء العديد من تلك المعايير والممارسات الجيدة لأمن المعلومات. وفيما يلي نستعرض بعض أعمال الهيئات المهنية، ومجموعات العمل للممارسين المتخصصين. مع التنويه إلى أنه كلما تتغير التكنولوجيات بسرعة، فإن أيا من هذه المعايير والممارسات لا يمكن عدها "نهائية". وبعض الفقرات الموجودة في القائمة التالية مقبولة ومطبقة على نطاق واسع بوصفها جيدة بما فيه الكفاية:

- مجموعة (ISO 27000) من المعايير لإدارة أمن المعلومات: تم نشر هذه الوثائق من قبل المنظمة الدولية للمعايير، يتم مراجعتها وتحديثها بانتظام.
- سلسلة وثائق (NIST SP800)، التي نشرتها شعبة أمن الحاسبات في المعهد الوطني الأمريكي للعلوم والتكنولوجيا. تتألف من أكثر من مائة وثيقة، وهذه السلسلة يتم أيضا تحديثها بانتظام.
- ومن المبادئ التوجيهية الأخرى ذات الصلة بالممارسات الجيدة والتي تغطي قطاعات أكثر تحديداً من ممارسة أمن المعلومات. نشير إلى الآتي:

- مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL) تغطي الأوصاف الشاملة للعملية. وتهدف إلى تحسين الاتساق مع تلك العمليات التي طبقت وتم تنفيذها. ويستخدم (ITIL) على نطاق واسع في جميع أنحاء العالم، وأسهمت في تطوير المعايير الدولية (20000 ISO) على إدارة خدمة تكنولوجيا المعلومات.
- أهداف الرقابة لتكنولوجيا المعلومات (COBIT)، الصادرة عن معهد حوكمة تكنولوجيا المعلومات (ITGI) وجمعية رقابة وتدقيق نظم المعلومات (ISACA). نطاقه الحالي يغطي الحوكمة، والتخطيط والتنظيم، واقتناء وتنفيذ وتقديم الخدمات ومتابعتها. ونشر الاصدار الخامس من (COBIT 5)، عام (2012)، ويشمل منشورات منفصلة مخصصة لأمن المعلومات.
- هيئة إدارة البيانات للمعارف (DMBOK). تتعامل مع جميع جوانب إدارة موارد البيانات. هذه القائمة ليست سوى "غيض من فيض". وعند تبني أي منها يجب أن يتم ذلك في ظل مراعاة استراتيجية أمن المعلومات للمنظمة وثقافتها ولغتها.

إن تبني وتطبيق أي من البنود أعلاه أو كلها يتطلب جهدا كبيراً من التعلم والتدريب يتبعها التزام بتغيير الممارسات اليومية والسعي للتحسين المستمر. التغيير مرحب به بالكاد، وفي أكثر الأحيان، يقاوم بقوة.

أسئلة الفصل

س (1): عرف حاكمية أمن المعلومات.

س (2): يؤكد المتخصصون على أن حاكمية أمن المعلومات هي أكثر من مجرد كونها وسيلة لادارة السجلات التقليدية.لماذا؟

س (3): ما هو الغرض من حاكمية أمن المعلومات.

س (4): ضع دائرة أمام الاجابة المناسبة

تعد حاكمية أمن المعلومات وسيلة مهمة في التعامل مع بيئة الاعمال اليوم لأنها ستسهم في:

A ـ خفض التكاليف بشكل عام وتكلفة المعلومات بخاصة	B ـ الحد من مخاطر إختراق أمن المعلومات
C ـ ضمان التعامل السليم مع برنامج أمن المعلومات	D ـ جميع ماذكر صحيح

س (5): وضح من خلال الشكل التساؤلات الثلاثة لادارة أمن المعلومات.

س (6): برأيك متى تنجز إدارة أمن المعلومات الأمور بشكل صحيح؟

س (7): كيف يمكنك أن تعرف أن إدارة أمن المعلومات تفعل الاشياء الصحيحة بالطريقة الصحيحة؟

س (8): برأيك ما هو الغرض من السؤال التالي: هل تفعل إدارة أمن المعلومات الأشياء الصحيحة بالطريقة الصحيحة جيدا بما فيه الكفاية؟

س (9): وضح من خلال الشكل أهم مكونات حاكمية أمن المعلومات.

س (10): ما المقصود بالاهداف الاستراتيجية الاستباقية لأمن المعلومات مع الاشارة إلى أهم هذه الاهداف.

س (11): ما المقصود باهداف رد الفعل الاستراتيجية لأمن المعلومات مع الاشارة إلى أهم هذه الاهداف.

س (12): تصف استراتيجيةأمن المعلومات كيفية تحول الادارة من حالة (كما هي) إلى حالة الوجهة/الهدف، كيف تفسر ذلك.

س (13): عرف سياسة أمن المعلومات.

س (14): وضح من خلال الشكل أنواع سياسات أمن المعلومات.

س (15): ما هو الهدف من سياسات أمن المعلومات.

س (16): بين من خلال الجدول أهم الحاجات المنظمية التي يفترض أن تعكسها سياسات أمن المعلومات.

س (17): عرف ثقافة المساءلة عن البيانات.

س (18): ضع دائرة أمام الاجابة المناسبة.

تشير ثقافة المساءلة عن البيانات ضمنياً إلى:

A ـ سرية البيانات	B ـ إتاحية البيانات
C ـ سلامة البيانات	D ـ حق البيانات

س (19): ضع دائرة أمام الاجابة المناسبة

لتعزيز ثقافة المساءلة عن البيانات يستلزم أن يكون كل فرد في المنظمة:

A ـ على بينة من أهميتها	B ـ مقتنعا بهذه الأهمية
C ـ يتحمل المسؤولية بشكل سليم	D ـ جميع ما ذكر صحيح

س (20): وضح دور التعليم في تفعيل برنامج حاكمية امن المعلومات.

س (21): ما ذا يعني القبول/ الايمان في اطار ثقافة المساءلة، وكيف يمكن تحقيقه.

س (22): تعد المسؤولية ركيزة اساسية من ركائز ثقافة المساءلة، لماذا ؟ وكيف يمكن تكريس إخلاقيات المسؤولية.

س (23): يرى المتخصصون أن برنامج حاكمية أمن المعلومات يمكن أن يفشل في التطبيق بسبب ضعف الاتصالات، قدم تفسيراً لذلك.

س (24): وضح من خلال الشكل السمات الاساسية لبيئة الوصول إلى المعلومات.

س (25): إذا كنت مسؤولاً عن إدارة امن المعلومات في المنظمة، كيف تقوم بتخصيص الموارد البشرية والمالية الضرورية لذلك؟

س (26): اختلف الكتاب بخصوص كيفية تحديد الدور الانسب لكبار موظفي أمن المعلومات، علق على هذه العبارة معززاً إجابتك بالشكل التوضيحي.

س (27): وضح من خلال الشكل الأدوار الخمسة للمدراء الآخرين في المنظمة والخاصة بأمن المعلومات.

س (28): لأجل تنمية الوعي الأمني ينبغي للافراد أن يدركوا ضرورة الحفاظ على أمن المعلومات، كيف يمكن تحقيق ذلك؟

س (29): تعد ادارة التهديدات الداخلية من صميم واجبات كل مدير، علق على ذلك.

س (30): لماذا يحصل الخطأ البشري في أمن المعلومات، وهل يمكن تداركه وكيف؟

س (31): ما المقصود بالنظافة الرقمية، وكيف يمكن تطبيقها في برنامج حاكمية أمن المعلومات؟

س (32): وضح من خلال الجدول أهم مبادئ حاكمية أمن المعلومات.

س (33): وضح من خلال الجدول أهم الشروط الضرورية للتطبيق السليم لمبادئ حاكمية أمن المعلومات.

س (34): إستعرض بعض أعمال الهيئات المهنية، ومجموعات العمل للممارسين المتخصصين الخاصة بمعايير وقواعد السلوك لأمن المعلومات.

س (35): أجب بوضع إشارة (صح) أو إشارة (خطأ) أمام العبارات الآتية:

	العبارات	الاشارة
1	تحدد حاكمية أمن المعلومات معايير إدارة المعلومات من قبل المنظمة، وتضمن التزامها بمجموعة كبيرة من الأنظمة العالمية والمحلية.	
2	هناك أدوار في أمن المعلومات يجب تنسيبها إلى الافراد خارج وظيفة تكنولوجيا المعلومات (خارجية أو داخلية) لتحديد احتياجات حساب الوصول، النظام والبيانات، والموافقة على الاستثناءات	

3	قرصنة الإنسان هي جزء لا يتجزأ من سمة الخداع والتلاعب في الطبيعة البشرية والممارسين الجيدين لا يحتاجون المهارات التقنية لكسر حواجز حماية أصول/ موجودات المعلومات	
4	المعايير والممارسات وقواعد السلوك الخاصة بأمن المعلومات يمكن عدها "نهائية".	

الفصل الرابع

التهديدات لأمن المعلومات

4

- تمهيد
- أولاً: تعريف التهديدات
- ثانياً: أنواع التهديدات
- ثالثاً: من الذي يسرق المعلومات وما هي أنواع المعلومات المستهدفة
- رابعاً: مجالات اختراق أمن المعلومات
- خامساً: تحديد نقاط الضعف

الفصل الرابع

التهديدات لأمن المعلومات

Information Security Threats

تمهيد:

تعد التهديدات لأمن المعلومات اليوم هي أكثر فتكا من العقد السابق. ولكي تواجه المنظمة التهديدات، يجب عليها أن تحدد أولا أنواع التهديدات لأمن المعلومات، من الذي يسرق المعلومات وما هي أنواع المعلومات التي تهمهم، ماهي الطرق التي يتم فيها فقدان المعلومات الحساسة، والمصادر الرئيسية لتهديدات أمن المعلومات.

أولاً: تعريف التهديدات

يمكن تعريف التهديدات بطرق مختلفة تنطوي جميعها على بعض القواسم المشتركة التي تجسد الاطار العام للتهديد بمفهومه الواسع، وفيما يأتي نستعرض نماذج من هذه التعريفات:

- هو الشخص، المنظمة، الآلية، أو الحدث الذي يمكن أن يلحق الضرر بالموارد المعلوماتية للمنظمة.
- أي ظرف أو حدث من المحتمل أن يؤثر سلبا على العمليات التنظيمية (بما في ذلك مهمة، وظيفة، صورة، أو سمعة)، الأصول التنظيمية

والأفراد والمنظمات الأخرى، أو للأمة من خلال تعديل المعلومات، و/ أو الحرمان من الخدمة.

- أنه " الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصياً كالمتجسس أو المجرم المحترف والقرصان المخترق أو شيئاً يهدد الأجهزة والبرامج والمعطيات أو حدثاً كالحريق وإنقطاع التيار الكهربائي والكوارث الطبيعية".

وفقا للتعاريف أعلاه يمكننا تحديد أهم أبعاد مفهوم التهديدات لأمن المعلومات على النحو التالي:

- توجد التهديدات متى ما وجدت نقاط الضعف ويمكن أن يكون هناك عدد من التهديدات لكل نقطة ضعف.
- تنبع التهديدات من " الأفعال والتصرفات المقصودة وغير المقصودة على السواء والتي قد تأتي من مصادر داخلية أو خارجية، كما أنها قد تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم الكفاءة اليومية المتوقعة. وقد تنبع أخطاء النظام من سوء إستخدام الأجهزة والبرمجيات، التحميل الزائد أو المشكلات التشغيلية وغير ذلك.
- قد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام، فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة، المتطفلين، الديدان، أو القنابل المنطقية، ...إلخ. والتي

تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة، إتلاف أو تحريف بياناته.

- يمكن تصنيف التهديدات في أنواع مختلفة بطرق مختلفة مثل التهديدات البشرية / غير البشرية، التهديدات المتعمدة /غيرالمتعمدة، تهديدات المهرة / غير المهرة، التهديدات الداخلية / الخارجية. الفيروس، على سبيل المثال، هو تهديد غير بشري، متعمد، عموما (في البداية على الأقل) وخارجي، ويمكن أن يكون تهديد المهرة أو غير المهرة (اعتمادا على مطور الفيروس). من ناحية أخرى، يوصف تهديد مدير النظم الساخط بأنه بشري، متعمد، ومهرة، وداخلي.
- التهديدات هي الأشياء التي يمكن أن تسبب الضرر، أو هي الأشياء السيئة المحتملة التي يمكن أن تحدث لأحد الأصول، ومن ثم يمثل خطراً ممكناً على النظام. وقد يكون هذا الخطر شخص يقوم بالتجسس أو التخريب، أو شيْ يحدث مشكلة في الحاسب وملحقاته، أو حدثاً مثل الحريق أو الفيضان، أو يستغل به نقطة ضعف النظام.

ثانياً: أنواع التهديدات

تتجسد أهمية تحديد أنواع التهديدات في أنه يساعد إدارة المنظمة في رسم ما يصطلح عليها" خارطة التهديدات لأمن المعلومات Information Security

Threats Map" ومن ثم تقييم مصادر التهديد، حيث أن من المهم النظر في جميع مصادر التهديد المحتملة التي يمكن أن تسبب ضررا لموارد المعلومات في المنظمة وفي كيفية التعامل معها، على النحو الذي يسهل معرفة وتحديد أي التهديدات الأكثر خطورة وبالتالي تركيز الرقابة على النشاط المرتبط به ومن ثم السعي الى تقليل الآثارالسلبية المحتملة له. حيث يمكن إستخدام أسس مختلفة في تصنيف التهديدات، وأهم هذه الأسس هي:

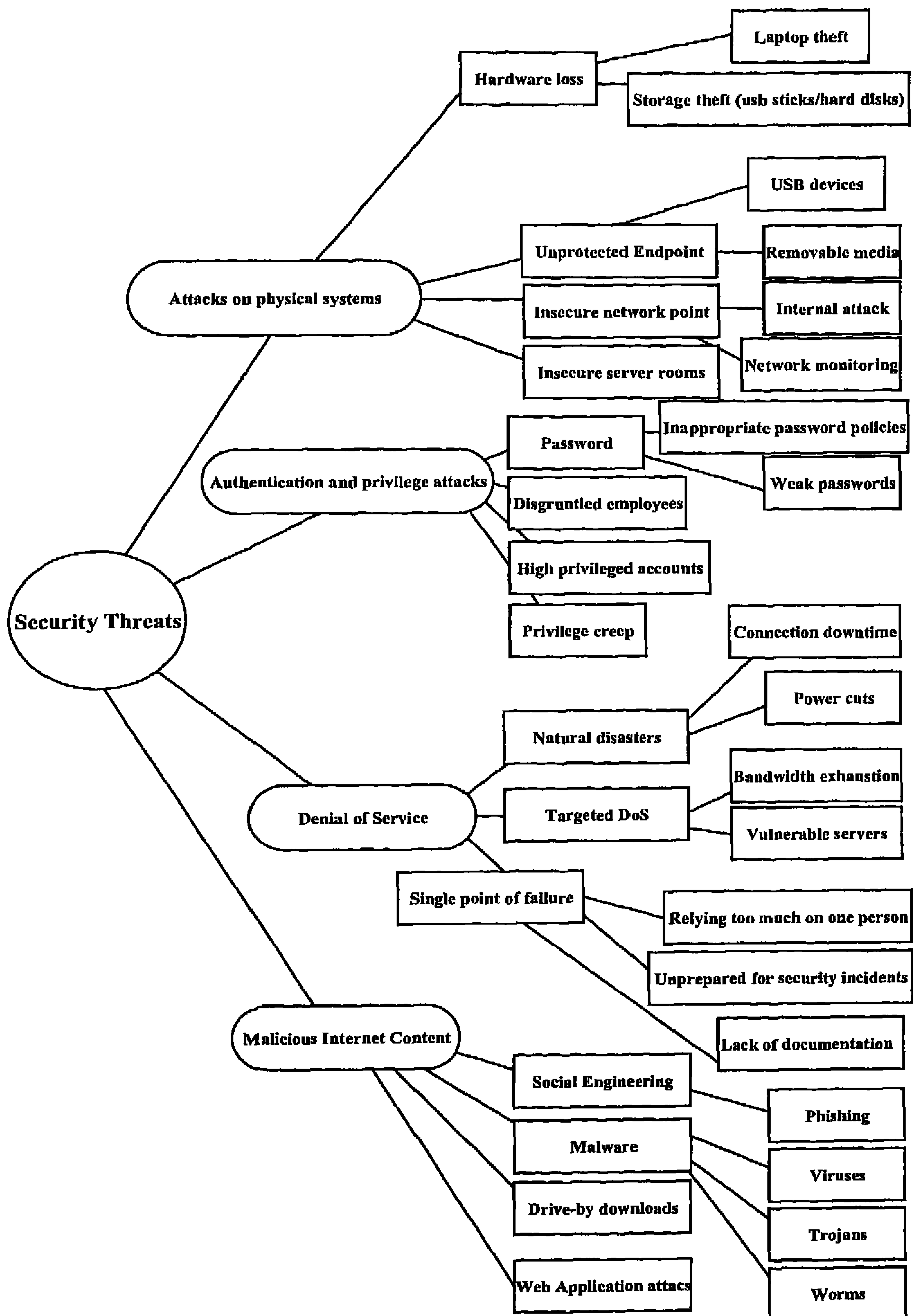
- نوع الهجوم المحتمل: يصنف الخبراء المختصين بالقضايا الأمنية عبر الشبكات والإنترنت التهديدات لأمن المعلومات الى نوعين من أنواع الهجوم المحتملة وهما: الهجوم التقني والهجوم غير التقني.
- حسب المصادر التي تنبع منها التهديدات: يرى (القحطاني والغثبر، 2009) إمكانية تصنيف التهديدات حسب المصادر التي تنبع منها الى نوعين وهما: مصادر تهديدات داخلية ومصادر تهديدات خارجية.
- حسب طبيعة التهديدات: يشير (**Stonebumer&Goguen&Feringa, 2002**) إلى أنه يتم تصنيف التهديدات حسب طبيعتها الى ثلاثة أنواع " تهديدات طبيعية، تهديدات بشرية، تهديدات بيئية".
- نوع الحدث الحاصل: يشير (الطيطي، 2010) الى أنه يمكن تقسيم أنواع التهديدات على أساس ما الذي يحدث مباشرة لأنظمة

المعلومات إلى أربعة أنواع ومن دون التطرق الى مصادر التهديدات وهي:

- الفضح والكشف Discloser.
- الوصول غير المصرح له للمعلومات Unauthorized Access to Information.
- الخداع Deception.
- التحكم غير الشرعي لأجزاء من النظام Unauthorized Control Of Some Part Of The System.

ويوضح الشكل (4 ــ 1) خارطة التهديدات لأمن المعلومات Information Security Threats Map، حيث تتضمن هذه الخارطة أربعة عناصر رئيسية تمثل مصادر للتهديدات لأمن المعلومات وهذه العناصر هي: الهجوم على الأنظمة المادية، الهجوم على حق التخويل والإمتيازات، إنكار الخدمة، البرمجيات الخبيثة، وكل عنصر من هذه العناصر بدوره يتفرع إلى مجموعة من العناصر الفرعية.

وفيما يأتي نوضح بايجاز أهم أنواع التهديدات المحتملة لأمن المعلومات من خلال تصنيفها الى تهديدات طبيعية و تهديدات بشرية، ومن أين تتبع هذه التهديدات، تهديدات داخلية أم خارجية. وتهديد الأحداث.



الشكل (4 ـ 1)
خريطة التهديدات لأمن المعلومات

1- التهديدات الطبيعية Natural Threats:

التهديدات الطبيعية يطلق عليها مفهوم آخر "الكوارث الطبيعية"، ويشير (داوود، 2000) الى أن الكارثة " أي حادث ينتج عنه تعطيل نظام الحاسب عن العمل لمده محسوسة"، ومن هذه التهديدات الطبيعية " الفيضانات، والزلازل، والأعاصير، والإنهيارات الثلجية والعواصف الكهربائية، وغيرها من مثل هذه الأحداث، وأشهر الكوارث الطبيعية على صعيد العالم، زلزال سان فرانسيسكو، وفيضانات بنغلاديش، وإعصار أندرو، وأخيراً زلزال تسونامي في اليابان في 11 أبريل 2012، والفيضانات التي حدثت في مدينة البندقية في إيطاليا في 12 نوفمبر 2012، وعادة أكثر ما يتضرر أثناء حدوث التهديدات الطبيعية في مجال أنظمة المعلومات هو النظام الذي ينهار في حدوث هذه الحالات، والأجهزة والمعدات الموجودة، وفقدان المعلومات الموجودة في الأنظمة. ونظراً لأن الكوارث الطبيعية " خارجة عن الإرادة البشرية، غالباً ما يكون فيها الدمار شاملاً وكبيراً، فإن التعاون بين الحكومة والقطاع الخاص والقطاع التطوعي، ينبغي أن يكون قائماً في إعادة الخدمة وإصلاح الأعطال.

2- التهديدات البشريةHuman Threats:

تعرف التهديدات البشرية بأنها " أي أحداث تتم عن طريق أخطاء البشر، مثل أعمال غير مقصودة (إدخال بيانات غير مقصودة) او إجراءات متعمدة مثل (الهجوم على الشبكة، تحميل البرمجيات الخبيثة، الوصول غير المصرح به إلى المعلومات السرية).

ويمكن تصنيف التهديدات البشرية إلى نوعين رئيسيين هما:

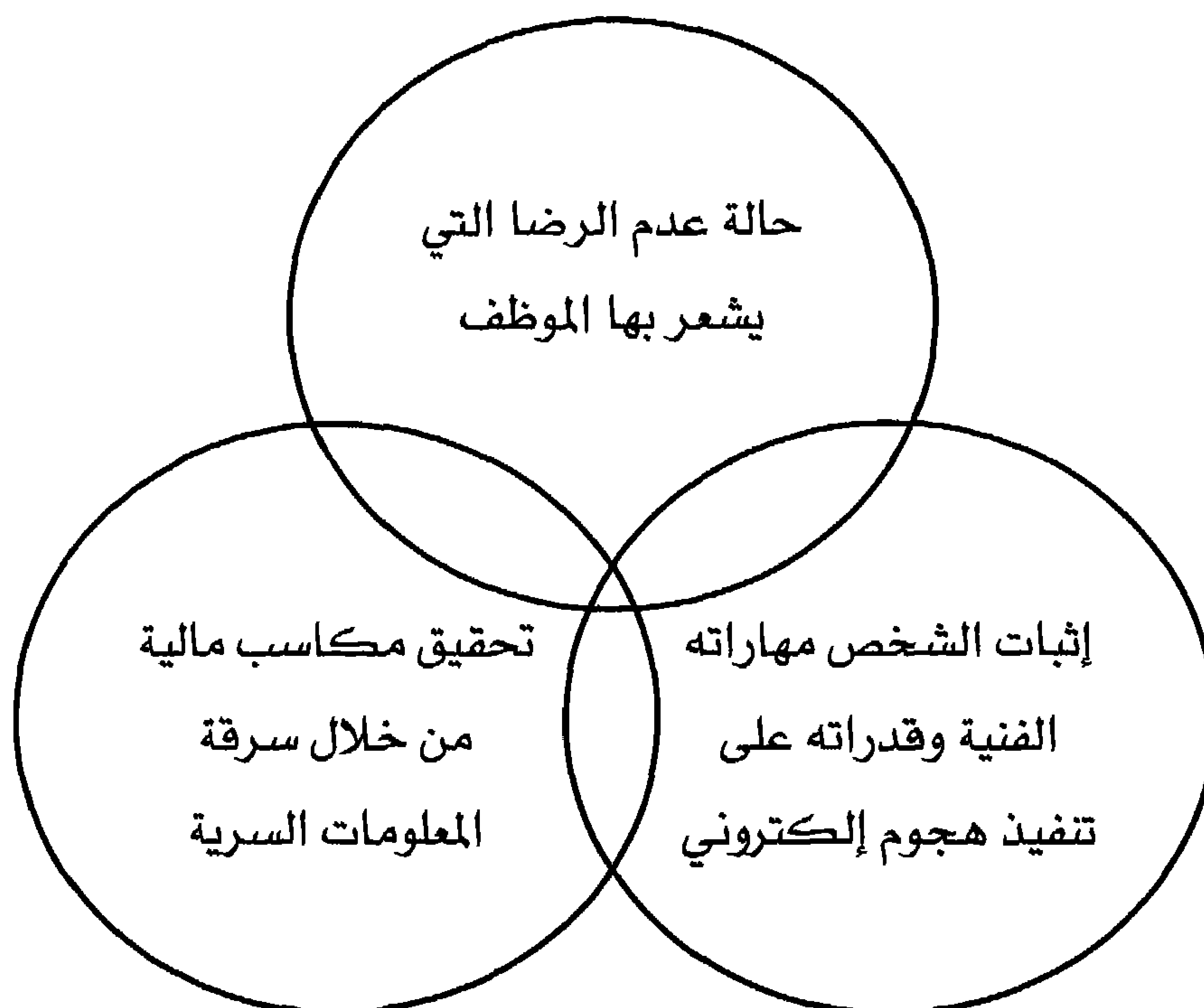
أ- المهاجمون من الداخل:

يؤكد (البداينة، 2002) بأن المسبب للتهديدات الأمنية هو الخطأ البشري، " يكون المعنى بذلك هم الموظفون والعاملون في المنظمة، إذ يشكل الموظفون ما نسبته (75 ـ 80٪) من مصادر التهديدات الداخلية في المنظمة وتشمل هذه الفئة الموظفين الحاليين والسابقين. المهاجمون من الداخل هم " أولئك الأفراد الذين ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية الى حماية أنظمة المعلومات التي تستخدمها تلك الجهة". " التهديد من الداخل ممكن أن يكون حدث ضار مقصود وغير مقصود، عن أشخاص متعمدين، الوصول إلى نظم المعلومات داخل المنظمة في الشبكة. والمهاجمون من الداخل كانوا دوماً الخطر الذي تواجهه أي جهة، مهما كانت سواء كانت تلك الجهة شركة أو منظمة أو حتى دولة. ومع إستخدام الحاسوب والتقنيات زاد الخطر الناجم عن الهجمات التي يقوم بها المهاجمون من الداخل ضد الجهة التي ينتمي اليها.

ويؤكد المتخصصون أن الهجوم من الداخل لا يحصل دون اسباب حقيقية، حيث أن هناك أسباب مختلفة للهجوم ضد نظم المعلومات، وهذه الاسباب يمكن إيجازها كالآتي: أنظر الشكل (4 ـ 2).

- حالة عدم الرضا التي تظهر عندما يشعر الموظف بعدم الرضا ومن ثم يقوم بمهاجمة نظم المعلومات للإنتقام.
- إثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم إلكتروني، حيث هناك بعض الأفراد يشعرون بالفخر والإعتزاز بنفسهم.

- تحقيق مكاسب مالية، حيث يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات سرية يستخدمها لاحقاً لابتزاز الجهة لدفع فدية مالية.



الشكل (4 ـ 2)

أسباب الهجوم من الداخل لأمن المعلومات

وقد يكون حجم التهديد الذي يمثلة هؤلاء المهاجمون من الداخل كبير بالنسبة للمؤسسة، والجدول الاتي يبين نماذج من التهديدات الداخلية.

1	إمكانية إلحاق الضرر بسرية المعلومات أو سلامتها.
2	إعاقة الوصول الى المعلومات أو منع الوصول للمعلومات.
3	إذا كانوا يمتلكون مهارة عالية بالتالي فإنهم يطمسون أي آثار تدل على إرتكابهم للهجوم.
4	إمكانية القيام بمهاجمة الشبكة الداخلية للمؤسسة التي يعملون فيها.
5	أيضاً إمكانية مهاجمة المعلومات بالسرقة أو التغيير أو الحذف.
6	فتح ثغرات في أنظمة الحماية التي تم وضعها لحماية أنظمة المعلومات فيها

الجدول (4 ـ 1)

نماذج من التهديدات الداخلية لأمن المعلومات

هنالك العديد من تلك الأخطاء التي تشكل تهديداً كبيراً على أمن المعلومات، و تشكل الأخطاء التقنية والتي حظيت بأكبر حصة، من بين أسوأ الأخطاء التي يرتكبها المستخدمون لأنظمة المعلومات ومنها:

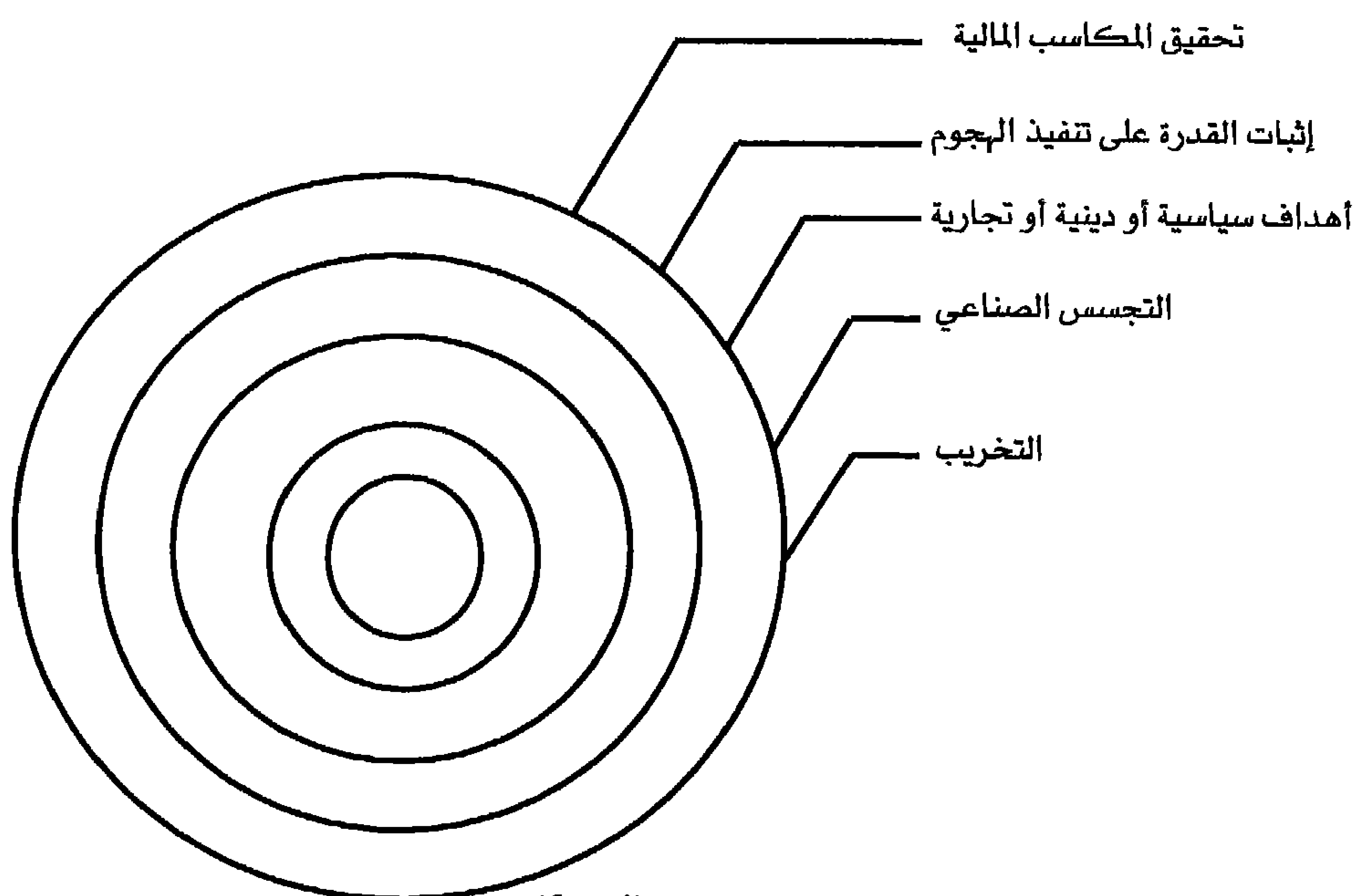
- عدم الاحتفاظ بنسخ إحتياطية وإختبارها.
- التصريح بكلمات مرور المستخدمين عبر الهاتف أو تغيير كلمات المرور بناء على طلب الأفراد عبر الهاتف ومن قبل أفراد لا يتم التحقق من هويتهم.
- عدم القيام بتحديث الأنظمة عند اكتشاف فجوات (ثغرات) أمنية فيها.
- ربط الأنظمة بالإنترنت قبل تشغيل أنظمة الحماية.
- الإستهانة بالمخلفات التقنية أمر بالغ الخطورة، إذ يقوم المهاجم بتفتيش المخلفات التقنية الخاصة بالمنظمة الموجودة في القمامة

والمواد المتروكة كمخلفات بحثاً عن أي شيء يساعده على إختراق النظام، مثل الأقراص الصلبة بعد استبدالها، أو الأوراق التي دون عليها كلمات السر أو أسماء الملفات والبرامج".

ب- المهاجمون من الخارج:

وهم " الأشخاص من خارج المنظمة والذين يطلق عليهم " القراصنة Hacker " والذين لديهم بواعث مختلفة للهجوم على الأنظمة، وهم أكثر خطورة من الموظفين الساخطين.

وفيما يتعلق بالبواعث التي يدفع بهؤلاء المهاجمين من خارج المنظمة، يشير المتخصصون هنا الى خمسة أنواع من البواعث هيكما موضحة في الشكل (4 ـ 3):

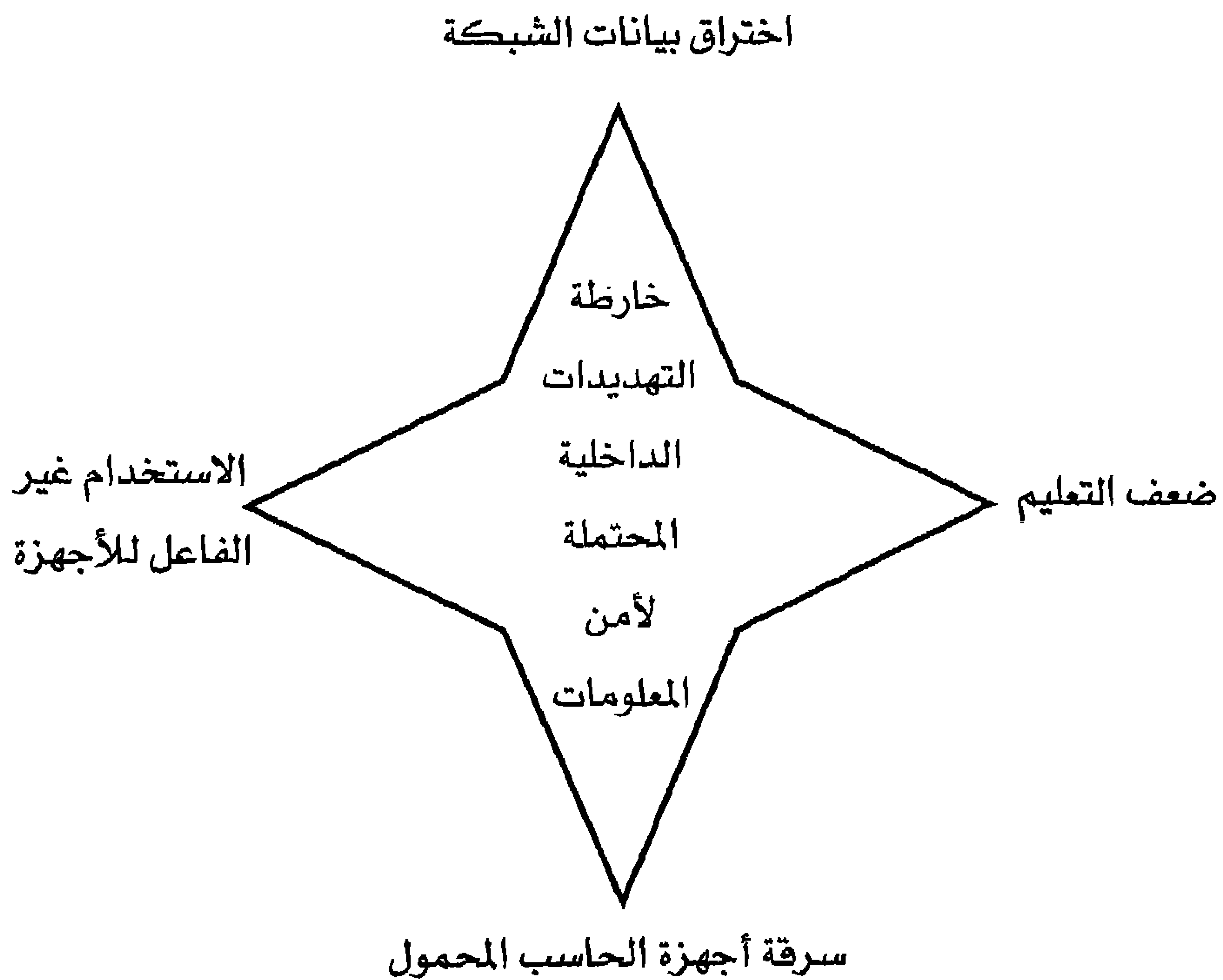


الشكل (4 ـ 3)

بواعث المهاجمين لأمن المعلومات من خارج المنظمة

3- التهديدات الداخلية:

وتشمل في المقام الأول الخروقات الأمنية العرضية الحاصلة من قبل الموظفين بسبب الاهمال أو غير المطابقة وسوء سلوك الموظف العامل على الأنظمة. ويشير (Sarkar,2010) الى خارطة التهديدات الداخلية المحتملة، وتحتوي على أربعة عناصر وهي إختراق بيانات الشبكة، الإستخدام غير الفعال للأجهزة، ضعف التعليم، سرقة أجهزة الحاسب المحمول (اللابتوب). ويوضح الشكل (4 ـ 4) هذه الخارطة.



الشكل (4- 4)

خارطة التهديدات الداخلية المحتملة لأمن المعلومات

4- التهديدات الخارجية:

وتـشمل في المقـام الأول تهديـدات الفيروسـات، وهجمـات القراصـنة، وإخفاقات البنية التحتية مثل الحرائق والهجمات الارهابية، هجمات الحرمان من الخدمة الموزعة، هجمات الاحتيال والبريد المزعج.

في حـين يبـدو أن معظـم المنظمـات علـى اسـتعداد لمواجهـة التهديـدات الخارجية، فإنها غير مستعدة بما فيه الكفاية لمواجهة التهديدات التي يحتمل أن تنشأ من داخل المنظمة. العوامل الداخلية عادة ما تكون الأكثر تجاهلاً عندما يتعلق الأمر بأمن المعلومات في المؤسسة. التهديدات الخارجية غالبا ما تلقى الكثير من الاهتمام عند إثارتها من قبل وسائل الاعلام وتصبح معروفة جيدا، مما يجعل من السهل للمنظمة التركيز عليها والتعامل معها. العوامل الداخلية عادة لا تكون قادرة على كسب الكثير من اهتمام وسائل الإعلام لسبب بسيط وهو لأنها يتم قمعها داخل المنظمة. ولسوء الحظ، لم يتم حتى الكشف عن بعض التهديدات الداخلية. ووفقا لمسح أمن المعلومات العالمية الذي انجز من قبل (Ernst & Young) عام(2004)، تم تصنيف حصان طروادة وديدان الانترنت كأكبر التهديدات. وجاء بالمرتبة الثانية التهديد المرتبط بسوء سلوك الموظف.

5- تهديد الأحداث:

ويمكن تصنيف التهديدات في الأنواع التالية:

أ- التهديدات الطبيعية:

يشار إليها في صناعة التأمين على أنها من فعل الله أو الطبيعة، مثل. الحرائق والفيضانات، الصاعقة، موجة المد والجزر، وثورة البركان؛

والزلازل، والأعاصير، والانهيارات الأرضية والانهيارات الثلجية والعواصف الكهربائية، وغيرها من مثل هذه الأحداث.

ب- **التهديدات العرضية:**

تصنف بدورها إلى:

- من فعل البشر: الذين يشاركون مباشرة، من خلال الأفعال غير العمدية، على سبيل المثال إسقاط شيء، التعثر على سلك الكهرباء، الفشل في تنفيذ إجراء يدوي بشكل صحيح، سوء ترميز المعلومات، miscuing، والفشل في عمل نسخة احتياطية، إدخال البيانات غير المقصود.
- من فعل غيرالبشر: على سبيل المثال، تسبب المتزلجين في انهيار جليدي، فشل التحويل بسبب قطع كابلات الكهرباء من قبل جرافة، والإعسار والإفلاس، أو سحب الدعم من قبل أحد الموردين الرئيسيين؛
- المعدات ومصممي المعدات: على سبيل المثال، عطل في القرص الصلب، فشل الكهرباء، علة البرمجيات، وفشل أجهزة تكييف الهواء

ج- **التهديدات المتعمدة:**

تصنف إلى:

- من فعل الإنسان: الذين يشاركون مباشرة، من خلال الإجراءات المتعمدة، على سبيل المثال، التخريب، الالتقاط المتعمد للبيانات غير الصحيحة، التعديل غير المبرر أو حذف البيانات، سرقة النسخة

الاحتياطية والابتزاز والتخريب، الهجمات على الشبكة، تحميل البرمجيات الخبيثة، والوصول غير المصرح به إلى المعلومات السرية

- من فعل غير البشر: على سبيل المثال، الكتابة على الجدران، التخريب، إطلاق سراح البرمجيات الخبيثة، الشغب والإرهاب والحرب.

وفيما يلي نستعرض بعضاً من التهديدات الأكثر شيوعا التي يواجهها أمن المعلومات والتي تقع ضمن فئة (فعل البشر المتعمد) وهي: القراصنة، المقنعون (masqueraders)، نشاط المستخدم غير المصرح به، التحميل دون حماية للملفات، وشبكات المناطق المحلية (LAN) وأحصنة طروادة.

- القراصنة: القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول للنظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطوري الأنظمة في النظام. وبالإضافة إلى ذلك، العديد من المتسللين هم بارعون في اكتشاف كلمات السر للمستخدمين المرخص لهم الذين يفشلون في اختيار كلمات المرور التي يصعب تخمينها أو تلك غير المدرجة في القاموس. تمثل أنشطة القراصنة تهديدات خطيرة للمعلومات السرية في أنظمة الحاسوب. حيث أنشأ العديد من المتسللين نسخ من الملفات ذات الحماية غير الكافية وتم وضعها في مجالات النظام والتي يمكن الوصول إليها من قبل الأشخاص غير مخولين.
- المقنعون (المتخفون): المقنع هو المستخدم المصرح به للنظام والذي حصل على كلمة مرور مستخدم آخر، على النحو الذي يمكنه

الوصول الى الملفات المتاحة للمستخدم الآخر. وهؤلاء المتخفون غالبا ما يكونوا قادرين على قراءة ونسخ الملفات السرية. والتنكر أمر شائع في الشركات التي تسمح للمستخدمين لتبادل كلمات السر.

- نشاط المستخدم غير المصرح: هذا النوع من النشاط يحدث عندما يحقق مستخدمي النظام المخولين الوصول إلى الملفات التي لا يحق لهم الوصول إليها. وضعف التحكم في الوصول غالبا ما يمكن من الوصول غير المصرح به، والتي يمكن أن تمس الملفات السرية.
- التحميل للملفات دون حماية: يمكن تحميل المعلومات السرية إذا تم في عملية التحميل، نقل الملفات من بيئة آمنة في الحاسبة المضيف إلى الحاسبات الصغيرة غير المحمية لغايات المعالجة المحلية. حيث يمكن الوصول الى المعلومات السرية غير المراقبة من قبل المستخدمين المصرح لهم على الحاسبات الصغيرة.
- شبكات المناطق المحلية: تشكل الشبكات المحلية تهديدا خاصاً للسرية بسبب أن البيانات التي تتدفق من خلال LAN يمكن مشاهدتها في أي عقدة في الشبكة، بغض النظر عما إذا كانت هذه البيانات معنونة أم لا إلى تلك العقدة. وهذا أمر مهم بشكل خاص لأن معرفات المستخدمين غير المشفرة وكلمات المرور السرية للمستخدمين الذي يسجلون الدخول إلى المضيف تخضع لتقديم تنازلات كلما تحولت هذه البيانات من عقدة المستخدم ومن خلال LAN إلى المضيف. أي معلومات سرية غير مخصصة للعرض في كل عقدة يجب أن تكون محمية من خلال التشفير.

- أحصنة طروادة: يمكن برمجة أحصنة طروادة لنسخ الملفات السرية إلى المناطق غير المحمية من النظام عندما يتم تنفيذ أية عملية من قبل المستخدمين الذين يؤذن لهم بالوصول إلى تلك الملفات. وحالما يتم التنفيذ، يصبح حصان طروادة مقيماً في نظام المستخدم، ويمكن نسخ الملفات السرية بشكل روتيني على الموارد غير المحمية.

ثالثاً: من الذي يسرق المعلومات، وما هي أنواع المعلومات المستهدفة؟

قد تؤدي الأحداث المهددة إلى الضرر. من الأصناف العامة للضرر هي الإصابات للأشخاص، إلحاق الضرر بالممتلكات، وفقدان قيمة الموجودات، وفقدان السمعة والثقة، و(الأهم) هو فقدان المعلومات، تحوير المعلومات، والوصول إلى المعلومات أو الكشف عنها، والنسخ من المعلومات. قد ينزعج أولئك الذين لا دراية لهم حتى الآن مع مدى التهديدات لأمن المعلومات في الذي يسرق المعلومات وأي نوع من المعلومات تهمه.

1- من الذي يسرق المعلومات؟

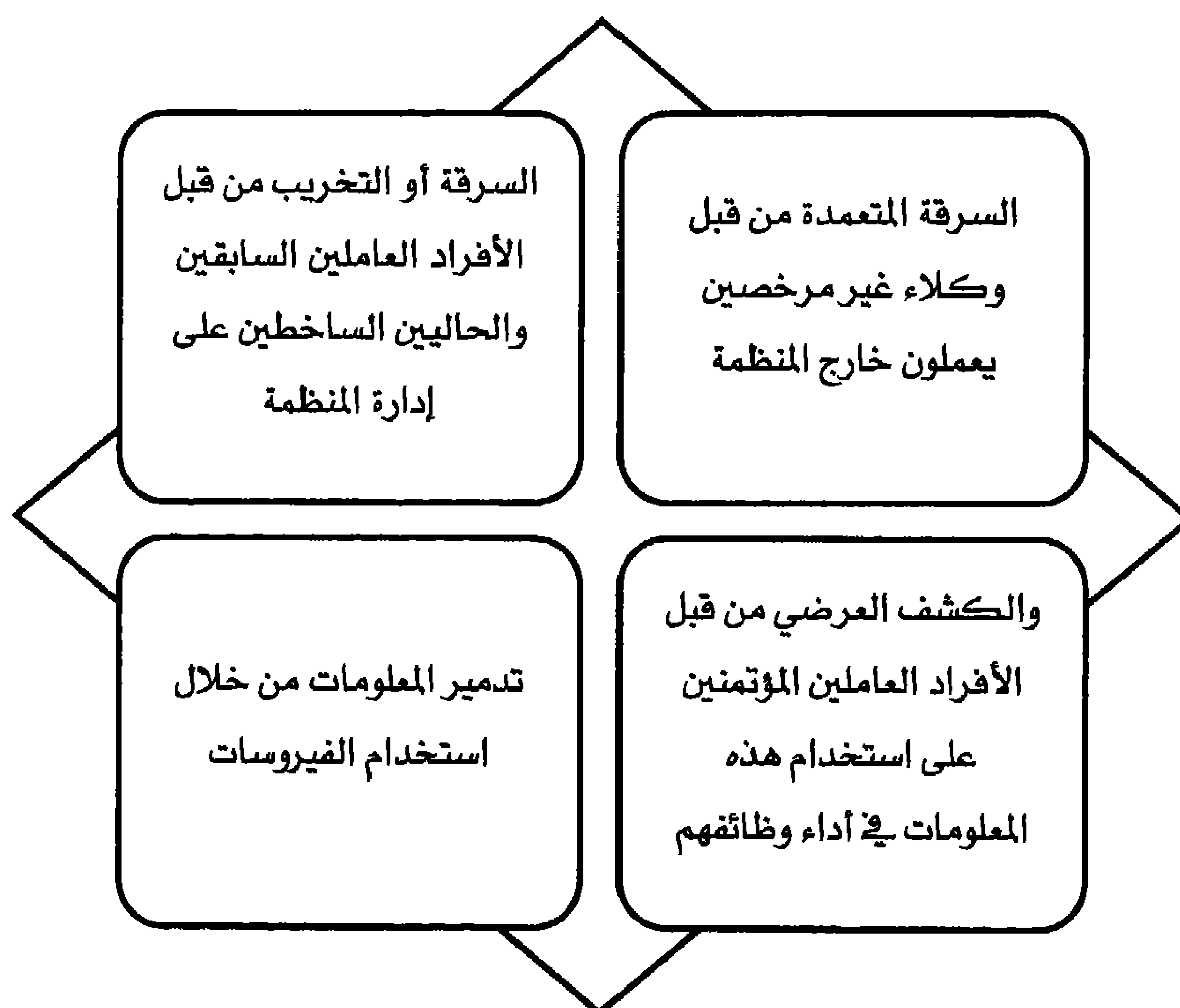
تتعدد الجهات التي تخترق أمن المعلومات إلى الحد الذي قد يتعذر معه أحيانا الكشف عن الجهة الحقيقية التي تقف وراء هذا الاختراق، ويشير الى هذه الحقيقة الباحث (Hill , 1995: 15) بقوله أن هؤلاء الذين لم يعتادوا على حجم المشكلات الملازمة لأمن المعلومات قد لا يمتلكون فكرة واضحة عن تلك الجهات التي تخترق أمن المعلومات، وهذه الجهات يمكن تعدادها على النحو الآتي:

الأفراد العاملون في مهام الاستلام والتسليم، المحققون، الزائرون بهدف الإطلاع، المستشارون، عملاء وجواسيس المنافسين، الأفراد العاملون حاضرا (المبرمجون، موظفي البريد، موظفي أمن المعلومات، البوابون)، زوجات الأفراد العاملين وأقربائهم، الأفراد الساخطون الذين انتهت علاقتهم بالمنظمة وطردوا من العمل.

2- ما هي أنواع المعلومات المستهدفة؟

أي شخص فعلياً، يمكنه الوصول من أي نوع إلى المنظمة قد يتسبب في حدوث خرق لأمن المعلومات. إذ تتباين الجوانب التي تثير الاهتمام لاختراق أمن المعلومات بتباين طبيعة المعلومات التي تكون عرضة للاختراق، ففي المستشفيات ينصب الاهتمام على سجلات المرضى، وفي مجال التسويق تكون استراتيجيات التسويق هي المهمة، وتستحوذ الأسرار الصناعية في العمليات الصناعية والإنتاجية على الاهتمام الأكبر. ويرى (Hill , 1995: 15-16) أن أهم الموارد المنظماتية التي تثير الاهتمام لسرقة المعلومات والتي يصطلح عليها (فقدان المعلومات الحساسة) هي: قوائم الزبائن، المعلومات المستنسخة، مراسلات المدير التنفيذي، بيانات البحث والتطوير، براءات الاختراع أو حقوق نشر المعلومات، مشاريع الموازنة، البيانات المالية، الصفقات القانونية، سجلات الأفراد، الخطط التسويقية. والسؤال الأول قد يسأله المسؤول التنفيذي هو " كيف خرجت المعلومات خارج المنظمة وأصبحت معروفة لأولئك الذين هم من غير المعنيين؟" للاجابة عن هذا السؤال وعلى الرغم من اختلاف الباحثين المختصين في مجال أمن المعلومات بخصوص الطرق التي يمكن من خلالها اختراق أمن المعلومات (عمار، **1990**) (منيب، **1990**) (قشقوش، **1992**)

(الشوا، 1994) (Ewing , 1992) (Tanzer , 1993) (Hill , 1995) (Parker , 1997)
إلا أن المعلومات يمكن أن تفقد بأربعة طرق رئيسة هي السرقة المتعمدة من قبل وكلاء غير مرخصين يعملون خارج المنظمة، السرقة أو التخريب من قبل الأفراد العاملين السابقين والحاليين الساخطين على إدارة المنظمة والكشف العرضي من قبل الأفراد العاملين المؤتمنين على استخدام هذه المعلومات في أداء وظائفهم، وأخيرا تدمير المعلومات من خلال استخدام الفيروسات، كما هو موضح في الشكل (4 ـ 5).



الشكل (4 ـ 5)

الطرق الرئيسة الاربعة لسرقة المعلومات

وفيما يأتي توضيحا لهذه الطرق:

أ- السرقة العمد:

وتتمثل في الاطلاع غير المخول به على المعلومات عن طريق الوكلاء غير المصرح بهم من خارج المنظمة. السرقة المتعمدة من الخارج، يصطلح عليها "التجسس الصناعي أو التنافسي" أو أكثر مجازا، " الاستخبارات التنافسية ". ووفقا لأحد الخبراء، فإن مثل هذا النشاط هو في ازدياد مستمر بسبب " تزايد حدة المنافسة العالمية بين المنظمات "، قصر دورة حياة المنتجات، إنخفاض هوامش الربح، وتراجع ولاءات الموظفين (**Tanzer, 1993**). إن القراصنة الذين يقتحمون نظم الحاسبات يبدون بريئون في سلوكهم كمحللي البحوث، محللي الأعمال والمتخصصين في المعلومات، والمشترين، الذين يكسبون ثقة الموظف من أجل الحصول على المعلومات السرية (**Marine, 1990**). ويأخذ هذا التجسس أشكالا عدة أهمها هي (**Abernathy,1991:77**):

- التقاط المعلومات التي تظهر على الشاشة المرتبطة بالحاسب من خلال الاطلاع عليها وهو ما يصطلح عليه بالالتقاط الذهني.
- التقاط المعلومات من خلال التصنت المجرد عليها بين الحاسب والمحطات الطرفية بوساطة خطوط تحويلية أو مرسلات صغيرة أو استخدام الهوائيات في حالة البث عبر الأقمار الاصطناعية.
- التقاط المعلومات مباشرة من الخطوط الهاتفية عن طريق وضع مركز تصنت أو مكبرات صوت صغيرة.

- التقاط المعلومات من خلال الإشعاعات الصادرة من الحاسب والأجهزة الملحقة به وفك رموز هذه الإشعاعات لتحويليها إلى اللغة الأصلية.
- التفتيش الدقيق في نفايات الشركات بحثا عن المعلومات.
- الدخول إلى النظم الحاسبية للمنظمة باعتماد ذرائع مختلفة مثل الادعاء بأنه باحث أكاديمي أو محلل شركات أو أخصائي معلومات أو مشتري يرغب بكسب ثقة الافراد العاملين.

ب- السرقة أو التخريب من قبل الموظفين السابقين أو الموظفين الحاليين الساخطين:

هي السرقة الداخلية للمعلومات، وتشير إلى الحالة التي تسخر وتوظف فيها المعلومات من قبل الموظفين الساخطين أو الموظفين السابقين لتحقيق أهداف غير مشروعة أو في مجالات غير مسموح بها لتحقيق مصالحه الشخصية أو مصالح جهات أخرى حتى في الحالات التي يحق للمستفيد في الوصول إلى هذه المعلومات. ويعد هذا النوع أيضا مقصوداً، هؤلاء الموظفين يسمحوا لأنفسهم باستغلالها في بعض الأحيان من قبل عناصر الاستخبارات التنافسية، إما من أجل المال أو لمجرد الرغبة في التجسس او بسبب طرد الفرد العامل ومن ثم قيامه بعرض معلوماته وكشف أسرار المنظمة واستراتيجيتها. على سبيل المثال، شخص ما تم تسريحه من العمل في المنظمة قد يذهب مباشرة إلى أكبر منافس لهذه المنظمة ويقوم في الكشف عن الأسرار التجارية، واستراتيجيات التسويق، أو خطط المنتج الجديد في كثير من

الأحيان على الرغم من الاتفاقات التي وقعت على عكس ذلك. وتأخذ هذه الطريقة صيغا عدة هي:

- سرقة المعلومات المخزونة في ذاكرة الحاسب أو في الأقراص والأشرطة من خلا استنساخها.
- زرع برنامج فرعي معروف لدى الفرد في البرنامج يتم إخفاءه بسرية تامة ومهارة لتحقيق أغراض غير مشروعة.
- التعديل في برامج الحاسب أثناء تصميم البرنامج او تنفيذه أو تحديثه وصيانته.
- استخدام الحاسب والمعلومات المخزونة فيه لارتكاب الخروقات وتنفيذها ومتابعة التنفيذ من خلال تصميم برنامج يخصص لهذا الغرض.
- إجراء تحويلات وهمية للنقود من خلال مستحقات مصطنعة.
- دفع مستحقات لشركات وهمية وتغذية الحاسب بقوائم دفع وهمية.
- استبدال رقم حساب بآخر أو إحلال بطاقة بأخرى أو مضاعفة الرواتب.
- طبع قوائم حسابات غير حقيقية واستغلال ثقة الزبائن بالحاسب.

ج- التعرض العرضي من قبل الموظفين المنوط بهم هذه المعلومات للاستخدام في وظائفهم الخاصة (Ewing, 1992):

الأسلوب الثالث من فقدان المعلومات، هو التعرض العرضي للمعلومات من قبل الموظف، ومن الواضح أنه التهديد الأكثر شيوعا. هذا النوع من الخرق الأمني هو عادة بسبب شيء أكثر من إهمال الموظف أو الجهل أو

اللامبالاة. هؤلاء الموظفين ببساطة لا يدركون أهمية الحفاظ على معلومات معينة آمنة. وأنهم ليسوا على بينة من العواقب الوخيمة في كثير من الأحيان والتي يمكن أن تنجم عند إغفال أمن المعلومات إلى جانب عدم معرفتهم المعلومات التي تحتاج إلى الحماية ومن يمتلك الدافع إلى سرقة هذه المعلومات من داخل المنظمة وخارجها وكيف يمكن كشفه وإيقافه في الوقت المناسب والتي تعتمد على طبيعة المعلومات بحد ذاتها وعلى نوع المنظمة، ويمكن أن تتراوح من مجرد الإحراج إلى فقدان مبالغ كبيرة من المال، أو حتى التهديدات للأمن القومي (Wood&Banks,1993:51)(Marine,1990: 24).

ج- تدمير المعلومات:

من خلال استخدام الفيروسات التي شغلت المتخصصين في السنوات الأخيرة بسبب اتساع مخاطرها وسهولة انتشارها والأضرار الكبيرة المترتبة عليها والتي تشتمل على مهاجمة البيانات والمعلومات والبرامج و إتلافها وحذفها وتعديلها جذريا من خلال تشويهها وتحريفها وإدخال معلومات غير صحيحة، حذف الملفات و إعادة تسميتها وتغيير تواريخ الملفات المخزونة، فضلا عن إيقاف الحاسب عن العمل او إبطاء تشغيله وتقليص السعة التخزينية. وتجدر الإشارة هنا الى صعوبة حصر وتعداد جميع أنواع الفيروسات المستخدمة حاليا في اختراق أمنية المعلومات وذلك لتعددها وتنوعها وتزايد انتشارها باطراد فضلا عن تطور صيغها وأشكالها باستمرار.

رابعاً: مجالات اختراق أمن المعلومات

تعد مجالات اختراق أمن المعلومات من اكثر الموضوعات مثاراً للجدل والاهتمام من قبل المختصين في نظم المعلومات بسبب كونها الأساس في توفير

الفرص الملائمة لحدوث الاختراق، وتتمثل هذه المجالات بالملفات الورقية، أجهزة الفاكس، الهاتف الخلوي، الثرثرة ، التجسس، انتحال الصفة وقواعد المعلومات الحاسبية، ونظم الاتصالات (Parker,1993:10-14). وهذه المجالات موضحة في الشكل (4 ـ 6).



الشكل (4 ـ 6)

مجالات اختراق أمن المعلومات

من هنا تقتضي الضرورة البحث في بعض الجوانب التفصيلية لهذه المجالات وعلى النحوالآتي:

1- **الملفات الورقية:**

على الرغم من استخدام النظم الحاسبية إلا أن الملفات الورقية لازالت تستحوذ على النسبة الأكبر من الملفات المستخدمة في اغلب المنظمات، واهم الفرص المتاحة في هذا المجال هي:

- عدم تصنيف الملفات على النحو الذي يمكن معه معرفة مدى سرية المعلومات التي تنطوي عليها ومن ثم حفظ هذه الملفات بشكل منفصل في مواقع أمينة أو في خزانات مقفلة.
- الاستعمال الواسع النطاق لأجهزة النسخ واستنساخ ما هو أكثر من النسخ المقررة سواء كانت المعلومات حساسة أم لا. أو محاولة بعض الأفراد نسخ صور من الوثائق الحساسة والاحتفاظ بها لأنفسهم، أو نسيان النسخة الأصلية في الجهاز.
- رمي النسخ الرديئة الطبع والتي تحتوي على معلومات حساسة دون تمزيقها بشكل ملائم.
- فشل إدارة المنظمة في التعامل مع البحوث الداخلية التي تنشرها المنظمة أو في جرائد أخبارها الداخلية او المجلات أو غيرها من النشرات التي تنشرها والتي قد تضم معلومات حساسة مثل إعلان الشروع بطرح منتج جديد أو نتائج البحوث التسويقية أو تفاصيل عن الأفراد العاملين في المناصب الحساسة.

- ضعف التعامل مع المعلومات التي انتفت الحاجة لها، إذ يتم على الأغلب التخلص منها من خلال رميها في سلة النفايات وهو أسلوب غير سليم، فقد تستغل هذه النفايات من قبل الأفراد الذين يتعاملون بها مثل الفراشين أو غيرهم لدوافع شخصية كما قد يندفع من يريد الحصول على المعلومات إلي البحث وبشكل قانوني وبقرار من المحكمة إلى هذه النفايات باعتبارها نفايات مهملة في مركز تجميع النفايات.
- اللجوء إلى طريقة بيع الأجهزة المنتهية والقديمة (Printouts)من ألحوا سيب والتي قد تضم معلومات سرية يتوجب عدم الاطلاع عليها.

2- وباء أجهزة الفاكس:

لقد ازداد استخدام هذه الأجهزة منذ منتصف الثمانينات وبشكل كبير بسبب المزايا العديدة التي تتصف بها والمتمثلة بالسرعة والسهولة العاليتين في نقل البيانات والمعلومات إلى جانب انخفاض التكلفة. ومع هذه المزايا فان هذه الأجهزة تتيح الفرص لاختراق أمنية المعلومات ومن أهمها:

- وضع هذه الأجهزة في مواقع عامة دون أية قيود تمنع الوصول إليها، بحيث يمكن لأي فرد عابر أن يضع لاقطة ناقلة أو البقاء أمام الجهاز والتقاط ما يسجله وخاصة في حالة ضعف الرقابة على هذه الأجهزة.
- الفرصة الأخرى تتمثل في الانتفاع من الخطوط الهاتفية التي يمكن اخذ خط منها بكل سهولة ومن ثم الوصول غير المرخص إلى

معلوماتها. وكما أشار أحد الخبراء فان بعض الحكومات تدخل روتينيا إلى كل الاتصالات الأجنبية القادمة وعندما تكتشف وجود بعض المعلومات المفيدة لشركاتها المورِدة المحلية فإنها غالبا ما تزود هذه الشركات بهذه المعلومات.

3- الهاتف النقال:

ازداد استخدام هذا الجهاز في السنوات القليلة الماضية بشكل مثير وخاصة من قبل رجال الأعمال لمزاياه الكثيرة المعروفة. إلا ان هذا الاستخدام يحمل في طيا ته فرصة خطيرة للاختراق من قبل المهتمين بالمعلومات المتدفقة عبر هذه الهواتف (**Menkus,1993:60**). إذ أن المعلومات السرية التي تنطوي عليها مكالماتهم ومناقشاتهم عبره واية معلومات خاصة بهم معرضة لاسترقاق السمع من قبل الأفراد الآخرين. فقد يلتقط أصحاب الهواتف الأخرى المكالمة أو يمكن التقاطها من خلال ما يسمى (Scanners) الخاصة بأجهزة الراديو عند ضبطها على التردد المناسب. يضاف الى ذلك فان العديد من أجهزة التلفاز ذات نظام (UHF) المصنوعة قبل عام 1982 قادرة على التقاط الترددات المستخدمة في الهواتف النقالة ولا يعرف كم هو عدد أجهزة التلفاز الموجودة تحت الاستخدام حاليا.

4- الثرثرة:

تعد الثرثرة من المجالات المهمة التي تتيح الفرص المناسبة لاختراق أمنية المعلومات وبخاصة في حالتين قد لا يأبه بهما الكثير من الأفراد العاملين وهما:

- المناقشات التي تجري في أوقات الراحة وتناول الطعام والشراب حول أعمال المنظمة والتي قد تكون منفذا لتسريب المعلومات إلى أفراد جالسين بالقرب منهم وينصتون لمناقشاتهم في الوقت الذي يتعذر معرفة هوية هؤلاء الأفراد المنصتين إذ قد يكونون على اتصال مع المنافسين ومن ثم تستغل هذه المعلومات للأضرار بالمنظمة.
- إغفال بعض الأفراد لأهمية السكوت وعدم الخوض في موضوعات قد تكشف بعض المعلومات الحساسة عن المنظمة وخاصة من قبل ممثليها في المحافل الرسمية أثناء السفر وحضور المؤتمرات والندوات واللقاءات الصحفية.

5- التجسس وانتحال الصفة:

ينطوي هذا المجال على فرص عدة متنوعة في أشكالها وفي أساليب استغلالها وهي فرص تتصف بشكل عام بكونها توفر الاطمئنان في نفوس الأفراد العاملين في المنظمة للتحدث وبكل سهولة عن المنظمة وتقديم المعلومات عنها. ومن نماذج هذه الأساليب نذكر:

- القيام بجولات سياحية استطلاعية لمشاهدة المعدات وعمليات الإنتاج.
- الادعاء بطلب الوظيفة والرغبة في التعيين في المنظمة ومن ثم ضرورة معرفة الكثير عن المنظمة من خلال المقابلات وإجراءات التعيين.
- الادعاء بأنهم باحثون أكاديميون او محللون صناعيين آو استشاريون أو طلبة وذلك من اجل الحصول على معلومات محددة عن المنظمة وأنشطتها والأفراد العاملين فيها.

- الادعاء بأنهم من كوادر الخدمات والتعيين في المنظمة كعمال للصيانة أو فراشين لجمع المعلومات من داخل المنظمة.

6- الملفات الإلكترونية:

كما هو الحال بالنسبة للملفات الورقية فان الهدف الأساس من أمن المعلومات للملفات الإلكترونية يتمثل في كيفية توفير الحماية للمعلومات التي تنطوي عليها هذه الملفات، وهي المسألة التي باتت الشغل الشاغل للمعنيين بها بسبب الفرص الكثيرة والسهلة التي يتيحها هذا المجال والتي يمكن الإشارة إلى بعض منها وهي:

- إساءة استخدام كلمة السر وتشتمل على (**Chebium,1991:32**):
  - إشراك الأفراد الآخرين في كلمات السر ومن ثم انتقالها إلى جهات أخرى تسعى إلى استغلالها ـ استخدام كلمات السر التي تحمل دلالات معينة في حياتهم اليومية مثل أسماء العائلة أو تواريخ الميلاد.
  - الاستمرار مدة طويلة دون تغيير لكلمات السر.
  - الاحتفاظ بنسخة مكتوبة من كلمات السر على المكاتب وبالقرب من أجهزة الحاسب.
- ترك المحطات الطرفية (**Terminals**) مفتوحة، إذ يلغي الحاجة إلى كلمة السر ويفتح المجال للوصول إلى المعلومات بكل سهولة.
- ترك أجهزة الحاسب المحمولة (**Laptop**) مفتوحة في غرف الفنادق أو على مقاعد الطائرات والقطارات ومترو الأنفاق بشكل يسمح

لمشاهدة ما يظهر على شاشاتها أو بوضع قرص مرن فيها واستنساخ المعلومات عليه (Menkus,1993:57).

- ترك حافظات الأقراص مفتوحة وخاصة تلك التي تضم معلومات حساسة الأمر الذي لا يتيح الفرص للاطلاع عليها أو سرقتها فحسب وإنما تعرضها إلى التلف بسبب تلاعب وعبث بعض الأفراد العاملين في محاولة لاستخدامها. ونفس الخطورة تكون قائمة عند غلق هذه الحافظات ولكن مع ترك المفتاح معلقا عليها.

7- نظام الاتصالات:

يمكن الاشارة الى الأنواع التالية:

- مراقبة الإتصالات: "بدون إختراق حاسب المجني عليه، يتمكن الجاني من الحصول على معلومات سرية غالباً ما تكون من المعلومات التي تسهل له مستقبلاً إختراق النظام".
- إعتراض الاتصالات: وهو "إعتراض المعطيات المنقولة وإجراء التعديلات التي تتناسب مع غرض الإعتداء"، و" يشمل إعتراض الإتصالات قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي".
- إنكار الخدمة Denial Of Service: "تحدث عندما يرسل المهاجم عدد كبير من طلبات الاتصال أو المعلومات إلى الهدف الذي سوف يعطل وبالتالي النظام لا يستجيب للطلبات المشروعة للخدمة"، ويتم من خلال " القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى

المعلومات أو الحصول على الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الالكتروني دفعة واحدة إلى موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته على إحتمالها أو توجيه عدد كبير من عناوين الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسلة فتؤدي إلى إكتظاظ الخادم وعدم قدرته على التعامل معه".

- عدم الإقرار بالقيام بالتصرف: يتمثل هذا الخطر في " عدم إقرار الشخص المرسل إليه أو المرسل بالتصرف الذي صدر عنه، كان ينكر أنه ليس هو شخصياً الذي قام بإرسال طلب الشراء عبر الإنترنت".

خامساً: تحديد نقاط الضعف Vulnerabilities

يجب أن يشتمل تحليل التهديدات لأمن المعلومات تحليلا لنقاط الضعف المرتبطة ببيئة أمن المعلومات بسبب أن مصدر التهديد لا يشكل خطراً عندما لا تكون هناك نقطة الضعف التي يمكن أن تستغل. ويمكن تعريف الضعف أيضا بطرق مختلفة:

- هو، عيب أو ضعف في إجراءات أمن المعلومات، والتصميم، والتنفيذ، أو الضوابط الداخلية التي يمكن أن تمارس (تسبب استغلالها عن قصد أو غير قصد)، ويؤدي إلى خرق أمني أو انتهاك لسياسة أمن المعلومات.
- هو، أي شيء يمكن أن تستغل لكسب أو رفض الوصول إلى أحد الأصول/ الموجودات أو خلاف ذلك تسوية الأصل.

- هـو، عمومـا عـدم وجـود حمايـة أو اسـتغلال شـيء مـا يمكـن استخدامه للوصول إلى أحد الأصول/ الموجودات.
- يشير الضعف إلى عدم القدرة على مقاومة بيئة معادية. الأشياء التي هـي من صنع الإنسان يتعذر أن تكون غير معرضة للخطر بنسبة (100٪). الى جانب ذلك، تكنولوجيات المعلومات تتعرض للفشل والتقادم.

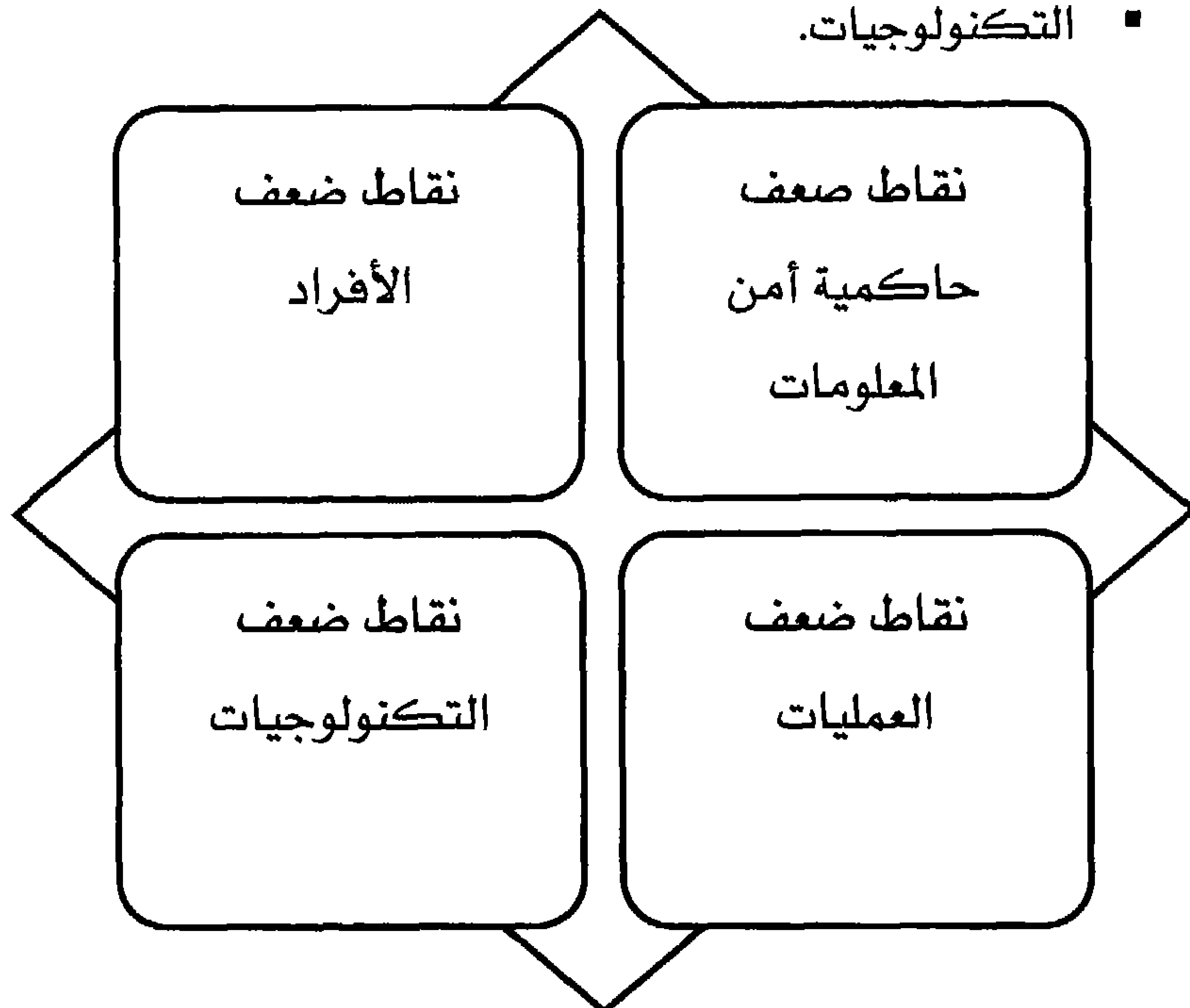
وفقا للتعاريف أعلاه يمكننا تحديد الأبعاد الرئيسية للضعف على النحو التالي:

- إذا تم وضع ضوابط ووسائل الحماية، لموقع معين سينخفض الضعف.
- الضوابط ليست جزءا من صيغة الخطر أعلاه، لكنها تؤخذ في الاعتبار لأن نقاط الضعف والضوابط هي طرق مختلفة حقا للنظر إلى الشيء نفسه.
- عندما تكون هناك ضوابط قوية، تكون نقاط الضعف قليلة، في المقابل، عندما تكون هناك نقاط ضعف كبيرة، تكون هناك عدد قليل من الضوابط القوية (بصفة عامة).
- في بعض الأحيان الضوابط قد تخفض أو تقضي على إحدى نقاط الضعف، ولكنها تخلق نقطة ضعف آخرى. على سبيل المثال، قد يكون حارس مسلح قادر على ردع معظم لصوص البنوك. ومع ذلك، يمكن للسارق الأعزل الذي يكون قادرا على التغلب على الحارس المسلح وسلب بندقيته، وبالتالي الحصول على مزيد من االقوة مما كان عليه من قبل. في هذه الحالة الثانية، إدخال الحراسة المسلحة (السيطرة) خفضت خطرأ واحداً ولكن خلق آخرجديد.

- الهدف من تحليل هشاشة الأوضاع هو وضع قائمة بنقاط ضعف أمن المعلومات (العيوب أو الضعف) التي يمكن استغلالها من قبل مصادر التهديد المحتملة.

ويصنف الكتاب نقاط الضعف التي قد تؤدي إلى الإخلال بأمن المعلومات في أربعة أبعاد هي كما موضحة في الشكل (4 ـ 7):

- حاكمية أمن المعلومات.
- الأفراد (إدارة تكنولوجيا المعلومات وغيرها).
- العمليات (في عمليات تكنولوجيا المعلومات، والتطبيقات، والدعم والبيانات وإدارة المشاريع، والاستجابة للحوادث والتعافي من الكوارث، واستمرارية الأعمال وإدارة الأزمات).
- التكنولوجيات.



الشكل (4 ـ 7)

نقاط الضعف التي قد تؤدي إلى الإخلال بأمن المعلومات

وفيما يأتي نستعرض بشكل موجز هذه الابعاد الاربعة لنقاط ضعف أمن المعلومات

1- نقاط ضعف حاكمية أمن المعلومات Governance vulnerabilities:

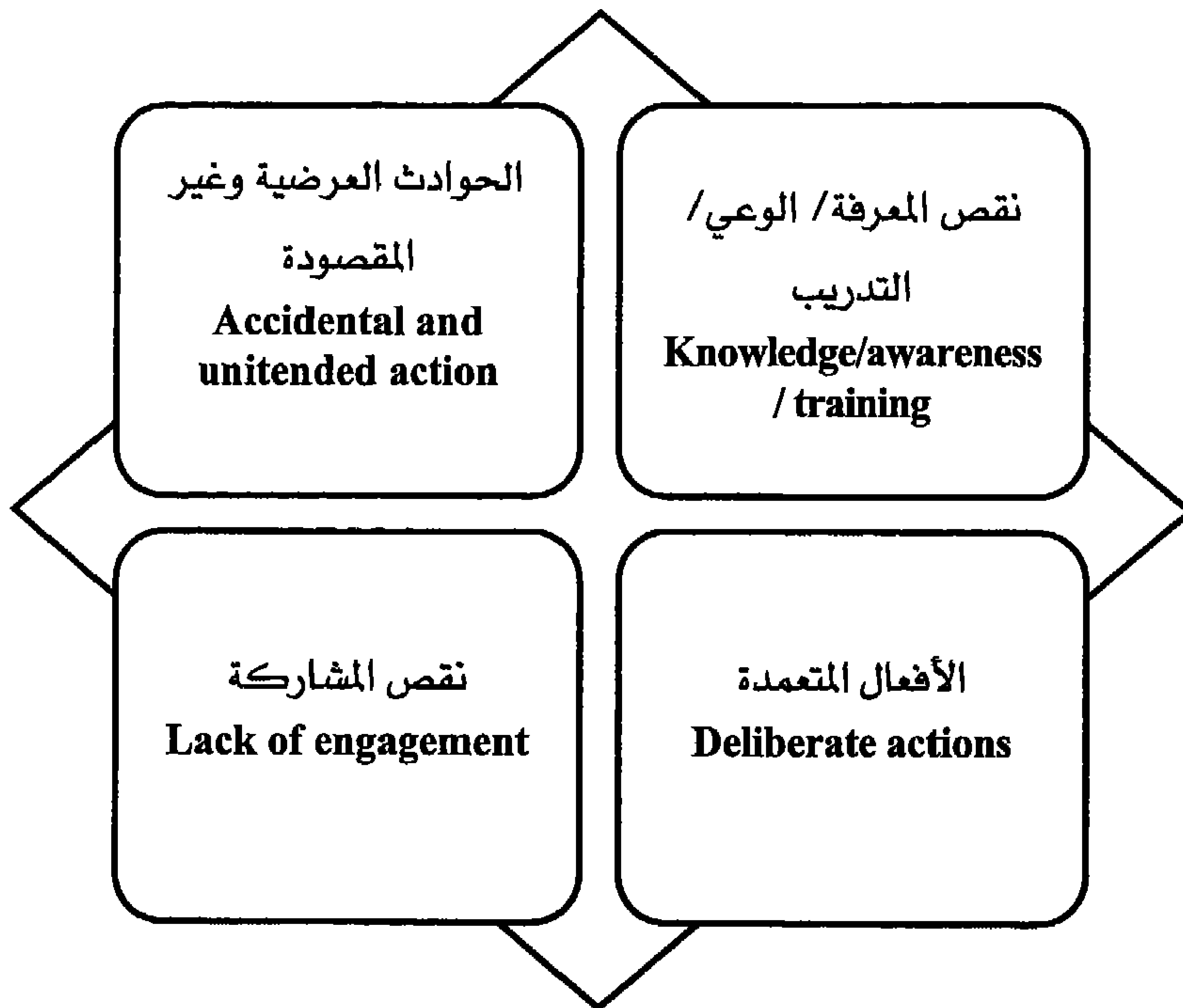
حاكمية أمن المعلومات (ISG) في كثير من الأحيان تكون أقل من ناجحة لعدد من الأسباب:

- التنفيذيين وكبار المديرين لديهم العديد من الموضوعات المتنوعة للتعامل معها ويواجهون مطالب ثقيلة في إطار الوقت المتاح لهم. وتضيف الحاكمية عبئاً إضافياً إلى عبء العمل الاعتيادي لهم، وتغطي موضوعا قد يكون غير مألوفاً لديهم. وبالتالي يتم إزاحتها من قبل أولويات أخرى.
- عدم القدرة على تقدير قيمة المعلومات والبيانات للمنظمة. على النحو الذي يمنع عقد مناقشة مستنيرة بشأن احتياجات الأمن والموارد التي ستخصص لهذا.
- كل منظمة لديها ثقافة فريدة من نوعها، والتي تشمل "السياسة". يمكن أن تسبب المشاكل عند تسعى المراكز الوظيفية لتعظيم نفوذها وميزانياتها.
- عدم الاستعداد لإنفاذ السياسات وفرضها، مما يجعلها عديمة الفائدة.

2- نقاط ضعف الأفراد People vulnerabilitie:

يسهم الأفراد بدور كبير في أنشطة أمن المعلومات، من بينهم نذكر المستخدمون النهائيون، مديري المشاريع ومنفذيها، المصممون (من جداول

البيانات البسيطة نسبيا الى البرمجيات والشبكات المعقدة)، الطالبين والمفوضون (لإنشاء حسابات وتحديد حقوق الوصول والامتيازات)، مالكي الأنظمة والبيانات (أو المؤتمنين)، الأدوار الفنية في تقديم الخدمات والدعم، مصممي الاستراتيجية والسياسة (على المستوى الوظيفي، مستوى الأقسام أو مستوى المؤسسة)، المشترين (الشركات والأفراد)، الاستشاريون و / أو مراجعي الحسابات، وأخرون. وتجدر الاشارة هنا الى أن نقاط الضعف المرتبطة بهذه الأدوار المختلفة تندرج تحت أربع فئات، كما هي موضحة في الشكل (4 ـ 8).



الشكل (4 ـ 8)

نقاط ضعف الأفراد العاملين ذات العلاقة بأمن المعلومات

أ- **نقص المعرفة / الوعي / التدريب:**

Lack of knowledge/awareness/training

إدارة أمن المعلومات وصيانته ليست مهمة سهلة التطبيق. ولكنها، وخلافا لمهمة قيادة السيارة التي تستلزم الحصول على رخصة القيادة، فإنها يمكن أن تطبق دون الحاجة إلى تقديم الشهادة أو الحصول على الترخيص. بعض التدابير الخاصة بتعزيز أمن المعلومات يمكن أن يكون آليا. ومن الأمثلة على ذلك الطلب من المستخدم النهائي تغيير كلمة المرور الخاصة به كل شهر. وهذا أمر جيد، ولكنه لا يعرف كيفية تصميم كلمة السر المناسب، فقد يحدد شخص ما الارقام ("123456") أو تاريخ الميلاد. الأسوأ من ذلك، عندما يحتاج الى عدة من كلمات السر المراد إنشاؤها والحفاظ عليها، فمن المرجح أن تكون مكتوبة أسفل الطاولة وحتى وضعها في مكان ظاهر مريح. وضع السياسات والمبادئ التوجيهية والممارسات الموصى بها في مكان ما في إنترانت الشركات هو أقل تكلفة من تقديم دورات التوعية، والبرامج التعليمية وغيرها من أشكال التدريب. بيد أن الضغوط للحد من النفقات جعل هذه المسألة هدفا سهلا لتخفيضات الميزانية.

ب- **الحوادث العرضية وغير المقصودة** Accidental and unintended actions:

حتى مع وجود أفضل فرصة تدريبية، الناس غير معصومون من وقوع حادث أمني بسبب خطأ بشري لا يمكن استبعاده. إذ يمكن أن تنشأ من خلال الضغط أخطاء للوفاء بمهلة، والإجهاد، والتعب، وعدم اتباع القواعد والسياسات، وما يمكن أن يكون الأفراد أيضا ضحايا للخداع والعمل ضد مصالح المنظمة، من خلال، على سبيل المثال، الكشف عن معلومات سرية.

خدمات مثل الرسائل النصية، المدونات ووسائل الاعلام الاجتماعية جعلت من السهل القيام به. الهندسة الاجتماعية في شكل الخداع ليس غير مألوف. شخص ما قد يدعي أنه يتصل من مكتب المساعدة لسؤال الفرد لتأكيد كلمة المرور الخاصة بهم. ويفعلون.

ج- **الأفعال المتعمدة** Deliberate actions:

القلق الراسخ: الفرد (الموظف، الاستشاري، المقاول، عامل النظافة، حارس أمن، الخ) يدفع للتحرك ضد المنظمة. الاحتيال، وسرقة الملكية الفكرية، والبيانات الفساد والتخريب والابتزاز، يحدث و في بعض الأحيان لن يتم الكشف عنها لفترة طويلة.

د- **نقص المشاركة** Lack of engagement:

نقطة الضعف الذي يصعب التعامل معها: الأفراد الذين لا يهتمون بأمن المعلومات، والمبادئ التوجيهية أو السياسات. الأفراد المحبطين أو الساخطين لمظالم حقيقية أو متصورة (مفترضة)، ينبغي اعتبار هؤلاء الأفراد بأنهم "سامة"، كما أن سلوكهم يمكن أن يكون معديا. عندما تجعل عقود عملهم وثقافة المنظمة من الصعب أو المستحيل فرض عقوبات على سلوكهم، فإنهم يمكن أن يصبحوا أكثر ثقة بأنفسهم

3- نقاط ضعف العمليات Process vulnerabilities:

هناك العديد من التعاريف لما نعنيه ب"العملية". لغايات هذا الكتاب، العملية هي: مجموعة من المهام ذات الصلة، التي نفذت من قبل الناس و / أو الأدوات التي تحول المدخلات إلى مخرجات. وينبغي إجراء العمليات بشكل منهجي لتحقيق الاتساق وإزالة الأخطاء وتحسين الدعم. وتم استخدام نموذج

نضج القدرة (Capability Maturity Model (CMM لتحديد المستوى الذي تم إضفاء الطابع الرسمي على العملية. وتم تحديد هذا النضج في خمسة مستويات:

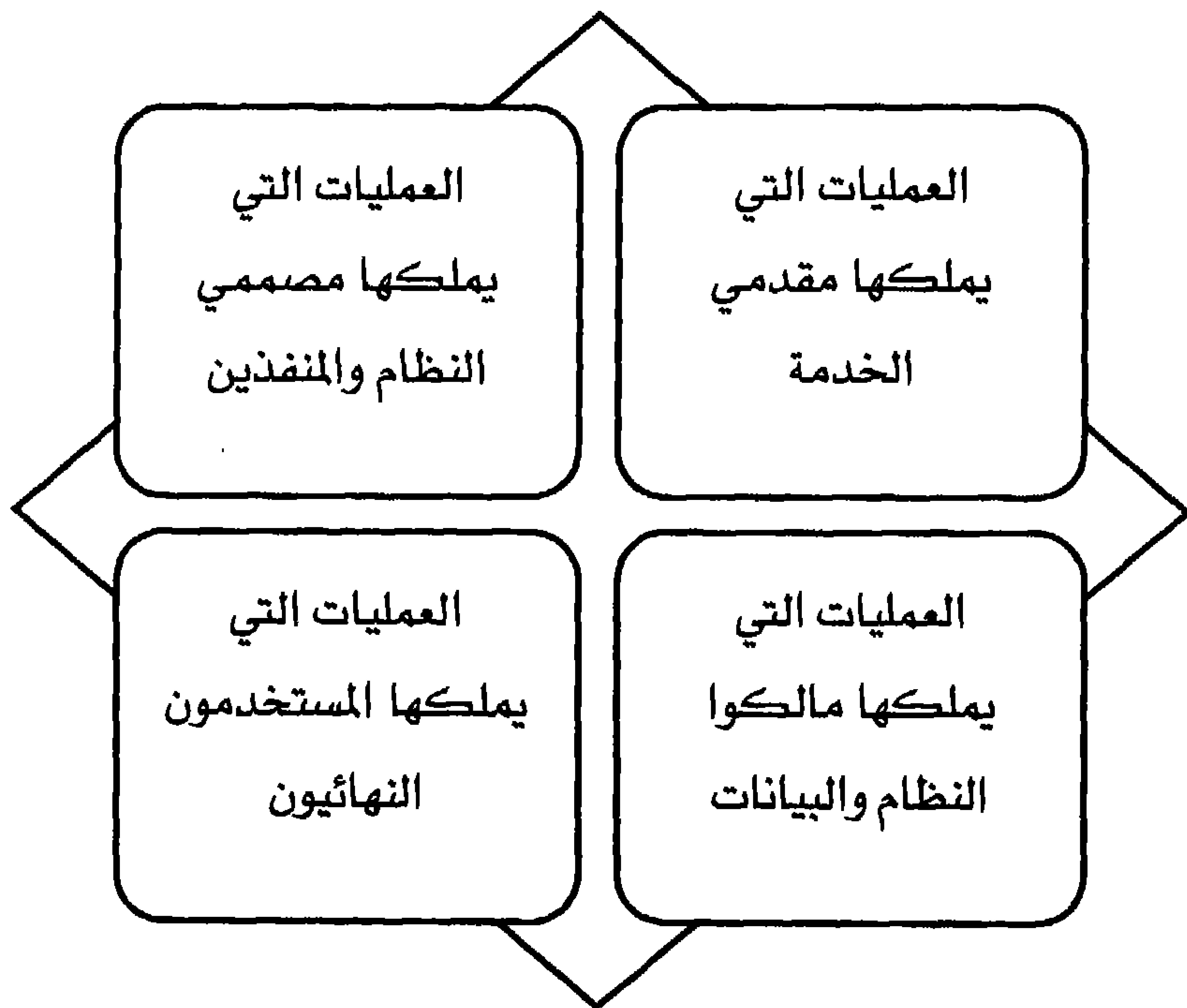
- الأولي: غير موثقة وعادة لن تتكرر(ويشار إليها أيضا بالفوضى أو المخصص)؛
- يمكن تكرارها: هذه العملية تم توثيقها إلى درجة أنه قد يكون من الممكن تكرار نفس الخطوات في كل مرة تتم فيها؛
- المحددة: تحدد العملية بالتفصيل من حيث تعليمات أو إجراءات العمل) وتنفذ باستمرار؛
- يمكن إدارتها: تتم إدارة العملية كميا مع المقاييس المتفق عليها؛
- يمكن تعظيمها: تدار العملية لتشمل التعظيم أو التحسين المستمر.

في حين أن مبادئ إدارة العملية بسيطة بما فيه الكفاية لفهما وإدراكها على نحو سليم، إلا أن مستويات النضج الأعلى لهذه العمليات يصعب تحقيقها، وذلك بسبب أنها تتطلب جهد متواصل على مدى فترة زمنية طويلة. التحدي في الحد من نقاط ضعف العملية يبدأ من خلال تحديد تلك العمليات التي تعد بالغة الأهمية (حرجة) لأمن المعلومات، وبعد أن تفعل ذلك، تبدأ بتبني المعايير والمبادئ التوجيهية والممارسات الجيدة التي تلائم على نحو أفضل ثقافة المنظمة واحتياجاتها. ويستلزم رسم الخرائط لمثل هذه العمليات مقابل احتياجات أمن المعلومات، النظر فيما يلي:

- العمليات التي يملكها مقدمي الخدمة (الاقسام الداخلية لتكنولوجيا المعلومات ومقدمي الخدمات الخارجيين)؛

- العمليات التي يملكها مصممي النظام والمنفذين؛
- العمليات التي يملكها مالكوا النظام والبيانات؛
- العمليات التي يملكها المستخدمون النهائيون.

والشكل الآتي يوضح خريطة العمليات المقابلة لاحتياجات أمن المعلومات.



الشكل (4 ـ 9)

خريطة العمليات المقابلة لاحتياجات أمن المعلومات

وفيما يأتي فكرة موجزة عن هذه العمليات:

أ- **العمليات التي يملكها مقدمو الخدمة:**

Processes owned by service providers

لا ينبغي أن تكون الإدارة معنية بتطبيق أي من الأطر المتاحة، ما لم تكن هناك مشاكل متكررة في الأداء و / أو توصيات من قبل المدقق بتسليط الضوء على مجالات محددة يوجد بها مخاطر. الممارسات الجيدة تؤسس لاتفاقات الخدمات الرسمية مع مقدمي الخدمة الداخلية التي تحدد أهداف الأداء وكيف سيتم قياس الأداء. إذا كان مقدم الخدمة خارجياً، فتكتب هذه الاتفاقات في عقود ملزمة قانونيا. هذه العقود أيضا تحدد أهداف الأداء، وكيف سيتم قياس الأداء والإبلاغ عنها وتطبيق الشروط الجزائية عند الفشل في الوصول الى المستويات المتفق عليها.

ب- **العمليات التي يملكها مصممو النظام والمنفذون:**

Processes owned by system designers and implementers

تطوير البرمجيات بدأت كحرفة وأصبح أكثر رسمية وهيكلية على مر السنين. وتم تأسيس نموذج دورة حياة تطوير البرمجيات (SDLC)على نحو جيد (هناك نماذج أخرى، مثل البرمجة الرشيقة). في الاساس ينطوي نموذج (SDLC) على أربعة مجالات رئيسية هي:

- التخطيط: يبدأ مع تحديد الحاجة، ,واختيار مجال التطبيق في المنظمة، ثم تحديد المتطلبات، تحديد ما إذا كان سيتم الشراء أو البناء، وطلب العروض، تقييمها، وما إلى ذلك، حتى يتم اتخاذ قرار.

- التطبيق: تطوير أو تكييف البرمجيات لتلبية الاحتياجات المحددة وتوثيقها واختبارها لدرجة أنها تصبح من الممكن دعم التغييرات والتحسينات في المستقبل.
- التوزيع: تحصل الموافقة على تأسيس البرمجية في بيئة الإنتاج لمزود الخدمة، ويخضع للصيانة (إزالة الأخطاء) ودعم المستخدمين النهائيين. عادة ما يتم ذلك من قبل البائعين أو الشركات المتخصصة، وهناك العديد من المبادئ التوجيهية والممارسات الجيدة التي تصف عمليات عديدة بالتفاصيل مع أهداف توفير ضمان الجودة والمستقبل
- الصيانة: من بين هذه المبادئ التوجيهية هي المجموعة المسماة هيئة هندسة البرمجيات للمعرفة (Software Engineering Body of Knowledge) المعروف إختصاراً (SWEBOK). هناك، أيضاً الكثير من المستخدمين النهائيين الذين وصلوا إلى درجة من الخبرة التي تمكنهم من تصميم وتنفيذ برامج متطورة (من جداول البيانات المعقدة إلى صفحات الويب) دون التفكير في مثل هذه الأنشطة على أنها تصميم برمجيات. ونتيجة لذلك، قد لا يتم اتباع الممارسات الجيدة، وربما لا تكون هذه البرمجيات موثقة أو تم إختبارها بالشكل الكافي. على الرغم من هذا، يتم إستخدامها من أجل دعم الأنشطة الحرجة والقرارات الحاسمة.

ج- العمليات التي يملكها مالكو النظام والبيانات:

Processes owned by system and data owners

تعد عملية إدارة الهوية والوصول إلى المعلومات أمراً أساسياً لحماية أمن المعلومات. فهي تحدد الأفراد الذين يحتاجون إلى حساب للوصول إلى نظم محددة حصرياً. وسيكون هناك مكتب مساعدة أو مجموعة مماثلة لإنشاء مثل هذه الحسابات لكن المساءلة عن الطلبات والموافقة على إنشائها، تعديلها أو إنهائها تبقى مع مالكي النظم. وينبغي أن تكون هذه الموافقات (أو الرفض) قابلة للارجاع. بعد إنشاء حساب للفرد، فإن الخطوة التالية هي تحديد ما هي البيانات التي يمكن له الوصول إليها وما العمليات التي يمكن أن يؤديها على تلك البيانات. على سبيل المثال، في الحسابات الدائنة، ينبغي أن لا يملك الموظف الوصول إلى سجلات الموارد البشرية. وبالمثل، ينبغي أن لا يملك موظف الرواتب صلاحية لتعديل الأجور لشخص ما دون ضوابط سليمة.

الحسابات والأذونات تحتاج إلى أن تدار من خلال دورة حياة تعكس التحركات الوظيفية، والترقيات، والإجراءات التأديبية، وما إلى ذلك، بدءاً من اليوم الذي تنشا فيه حتى يترك الفرد المنظمة. تظهر نقاط الضعف عندما يتم ترك هذه الأنشطة "ليوم آخر for another day" بسبب الأولويات الأخرى أو الضغوط للحد من التكاليف. تقع العمليات ذات الصلة بالبيانات في ثلاث فئات هي: جودة البيانات، وتصنيف البيانات ونظام الأذونات. وبينما تعد جودة البيانات، أساسية، إلا أن لها تأثيراً محدوداً على أمن المعلومات. بالمقابل يرتبط تصنيف البيانات ارتباطا وثيقا بالسرية. فالتصنيف يفرض على مالكي البيانات تنسيب البيانات إلى فئة في مجموعة بحيث تطبق في المنظمة

بأكملها. هناك تسميات نموذجية لهذه الفئات تشمل سرية للغاية، سرية، محجوبة، محظورة حتى، والعامة. فشل تصنيف البيانات يعني دعوة من أجل أن ترك المنظمة دون رقابة مناسبة.

د- العمليات التي يملكها المستخدمون النهائيون:

Processes owned by end users

لقد أدت زيادة شعبية الأجهزة الصغيرة والقوية (أجهزة االحاسب خفيفة الوزن، وأجهزة الحاسب المحمولة، والأقراص والهواتف الذكية) والتبني السريع لها من قبل السكان عموما جنبا إلى جنب مع الاتجاه لاستخدام مثل هذه الأجهزة الشخصية في بيئة العمل تحت شعار - "أحضر جهازك الخاص بك" الى تأكيد الحاجة إلى أن تكون العمليات الأمنية مملوكة من قبل المستخدمين النهائيين بغض النظر عما إذا كانت هذه الأجهزة تخزن فيها البيانات الحساسة أو يمكنها الوصول الى هذه البيانات. بينما يجب أن تكون الأساسيات، مثل الاستمرار في تحديث البرامجية، استخدام البرمجيات المضادة للفيروسات، عمل نسخ احتياطية من البيانات، وما إلى ذلك، معروفا جيدا، إلا أنه في الواقع قد لا يكون هذا هو الحال. إذ يبدو أن العديد من الناس غير مكترثين حول مخاطر عدم القيام بذلك. وبالإضافة إلى ذلك، فإن الشبكات الاجتماعية وتحميل البرمجيات المجانية أو منخفضة التكلفة، وخاصة تطبيقات لهواتف الذكية والأجهزة اللوحية، جميعها أدخلت مخاطر جديدة.

4- نقاط الضعف التكنولوجية Technology vulnerabilities:

التقنيات هي عرضة للفشل. قد يكون هذا تدريجياً، كما هو الحال عندما يتآكل الجسر، أو مفاجئاً: في حال انطفأت الانوار. قد يكون الحل من خلال عمل الصيانة وقد يكون قابل للإصلاح. لكن ليس دائما، حيث أن الضرر قد يكون كبير جدا (مثل محطات الطاقة النووية في فوكوشيما) ويصبح لا رجعة فيه.

إن الفشل في تكنولوجيات المعلومات نادراً ما يكون تدريجياً. فشل الأجهزة غالباً ما يكون قابل للإصلاح، ولكن ليس دائما: إذا تعرضت غرفة الكمبيوتر الى حريق (أو الفيضانات) فقد تتطلب استبدال جميع المعدات. فشل البرمجيات بسبب أخطاء التصميم قابل للإصلاح إذا ما توفر الوقت والخبرة. الفشل نتيجة لهجوم عبر الانترنت يسبب عواقب لا يمكن التنبؤ بها: حدث هجوم عبر الانترنت على النظم الإدارية لشركة آرامكو السعودية في أكتوبر 2012 وأصاب 30.000 جهاز كمبيوتر ومسح جميع البيانات الخاصة بهم. تنظيف واختبار كل هذه الحواسيب 30.000 وإعادة البيانات الخاصة بهم (أو على الأقل جزء منها) تم إعتباره من المشاريع الكبيرة.

أ- انعدام الأمن بوساطة التصميم - الدروس التي يمكن استخلاصها من الصناعات الآمنة:

Lack of security by design – lessons to be learned from the safety industry

أصبح أمن المعلومات مصدر قلق دائم. في الأيام الأولى من الحوسبة، كان التركيز على عناصر التحكم في الصلاحيات لعدد قليل من الناس.

وعندما ظهرت أجهزة الحاسبات الشخصية في السبعينات, كانت في المقام الأول للهواة وغالباً للأشخاص المهتمين بتكنولوجيا المعلومات والاتصالات، ولم تنتشر في المنظمات حتى منتصف الثمانينات. إلا أن التصميم الأساسي لمثل هذه الحاسبات لا تشمل ميزات الأمان. ثم ظهرت البرمجيات الخبيثة بعد سنوات قليلة واستخدمت كلمة "فيروس" في عام(1984) وفي البداية كان أساساً مصدر ازعاج. كانت أجهزة الحاسبات الشخصية لا شبكية والفيروسات تنتشر من خلال تبادل الأقراص المرنة. لا تزال التصاميم الحالية تتطلب من المستخدم للحصول على منتجات إضافية (مثل مكافحة الفيروسات، والتشفير، وخزائن الوثائق الإلكترونية").

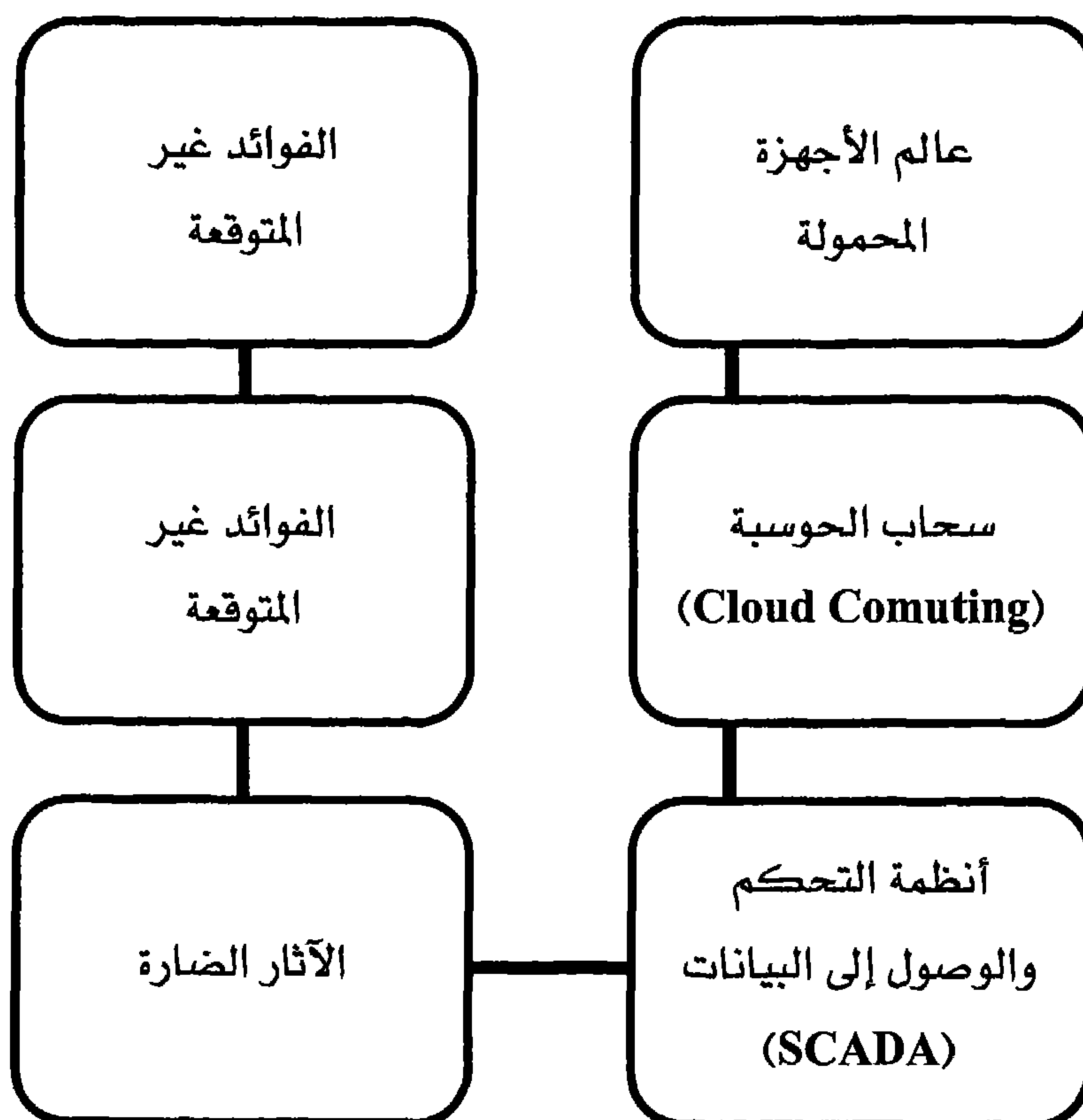
وبعدها بدأ العمل نحو ما نسميه الآن شبكة الإنترنت في منتصف الستينات كشبكة مقيدة، لم يتوقع مصمميها أنها سوف تصبح شبكة عالمية ذات آثار أمنية كبيرة. تم اكتشاف تأثير البرمجيات الخبيثة على شبكة الإنترنت في عام (1988)، عندما كتب طالب برنامج أسماه (دودة موريس) ينتشر بسرعة من خلال شبكة الإنترنت وتسبب في توقفها عن العمل. يشتهر المصمم لهذا البرنامج بمقولة: "لو أنني جربته على جهاز محاكاة أولاً".

تلاها ظهور الهواتف المحمولة في عام (1973) كجهاز محمول لإجراء المكالمات الصوتية. وتطورت الى "الهواتف الذكية" و "أقراص" وأجهزة ذات مواصفات عالية مثل أجهزة الكمبيوتر الشخصية، ولا تتضمن هذه الأجهزة الأمن بوصفه جزءاً لا يتجزأ من تصميمها بخلاف ذلك، ربما تتطلب استخدام أربعة أرقام للتعريف الشخصي.

صناعة السلامة، وجدت في الصناعات الاستخراجية، والبناء، والنقل، والصناعة التحويلية، والرعاية الصحية وغيرها، ويتم التعلم من التجربة. وجهات نظرهم هي أن الممارسات السيئة موجودة وتؤدي إلى أخطاء معروفة، على سبيل المثال المطرقة التي تسقط من أعلى السقالات ولكن لا تؤذي أحدا. ونادرا ما تحدث هذه الأخطاء. "الحظ" يكون كما ما هو عليه، لا يعمل دائما لصالح المنظمة وتحدث حوادث طفيفة على أساس منتظم. يتم الإبلاغ عن هذه الحوادث وتصبح جزءا من السلامة في إحصاءات العمل. من وقت لآخر، يحدث حادث كبير، يقوم المسؤولون عن صناعة السلامة على الفور بالتحقيقات لتحديد السبب الجذري واتخاذ خطوات لإزالته. ويتم اختبار هذه التعديلات على نطاق واسع قبل ان يتم التشغيل مرة أخرى. مثال في عام 2013 ينطوي على أسطول كامل من الطائرات الجديدة (بوينغ 787) التي كانت على الارض لعدة أشهر حتى تم اختبار التصميم وعمل التعديلات اللازمة كي يرضي سلطات التصديق. ولكن الحال مختلف في الوقت الحاضر في صناعة تكنولوجيا المعلومات.

ب- العواقب غير المقصودة:

مفهوم "عواقب غير مقصودة" يعود إلى أواخر عام 1700. ويشمل هذا المفهوم الفوائد، والآثار الجانبية السلبية أو الضارة التي حدثت عن دون قصد. الابتكار في تكنولوجيات المعلومات جلب معه ستة أنواع من الفوائد، والآثار الجانبية السلبية، كما هي موضحة في الشكل (4 ـ 10).



الشكل (4 ـ 10)

العواقب غير المقصودة لتكنولوجيا المعلومات والاتصالات

وفيما يلي نوضح بايجازهذه الأنواع الستة من العواقب غير المقصودة لتكنولوجيا المعلومات والاتصالات:

- الفوائد غير المتوقعة: وهي القدرة على ربط العالم، وتوفر سهولة الوصول إلى المعلومات والخدمات وأوجدت أشكال جديدة من وسائل الترفيه والأعمال.

- الآثار الجانبية السلبية: وتشمل ظهور وانتشار البرامج الضارة، على قدر من فقدان الخصوصية والعديد من الفرص لإضاعة الوقت.
- الآثار الضارة: تشمل جميع أشكال الجريمة الإلكترونية والهجمات الناجحة على البنى التحتية الحساسة، وسرقة الملكية الفكرية ويحتمل أن تكون شكل من الأشكال الجديدة للحروب.

وهناك ثلاث أنواع إضافية من نقاط الضعف التي تستحق اهتمام الإدارة والتي تندرج أيضاً ضمن العواقب غير المقصودة وهي SCADA، والحوسبة السحابية والأجهزة النقالة:

- أنظمة التحكم والوصول إلى البيانات (**SCADA**): أجهزة وشبكات التواصل مع العالم المادي بدءا من ضوابط بسيطة نسبيا من ظروف الهواء والمصاعد، الدائرة المغلقة للتلفزيون وأجهزة الاستشعار في المراقبة، وأجهزة الصراف الآلي، وما إلى ذلك من النظم الموزعة المعقدة في السيطرة على عمليات التصنيع والمرافق والنقل. هذه نادرا ما تكون مسؤولية تكنولوجيا المعلومات ومصممة للتبسيط وزيادة الموثوقية في هذه التطبيقات، وليس لحماية أمن المعلومات.
- سحابة الحوسبة (**Cloud Computing**): هو الوصف المختصر للموارد المحوسبة التي يتم استخدامها عن طريق شبكة الإنترنت. في هذه البيئة تدار أجهزة الحاسبات والبرمجيات من قبل طرف ثالث ويتم مشاركتها بين العديد من العملاء. هذا يقدم البساطة وانخفاض التكاليف من خلال عدم وجود البنية الأساسية داخل

الشركة. إذا تم فقد الاتصال بالإنترنت لأي سبب من الأسباب مثل الهجمات على خطوط الشبكة فإن جميع الخدمات المقدمة من خلال السحب لن تكون متوفرة حتى يتم إصلاح الانقطاع.

- عالم الأجهزة المحمولة: يخضع للتحديات الجديدة التي تتراوح بين البرمجيات الضارة التي تستهدفه، وسرقة البيانات، وفقدان أو سرقة الأجهزة، وبشكل متزايد، وقضايا أخرى تظهر في كل وقت، مثل القدرة على تحديد الموقع الجغرافي للفرد من خلال أجهزتهم بحيث يخلق أنواع من المخاطر التي لا تزال غير مفهومة تماما.

أسئلة الفصل

س (1): عرف التهديد.

س (2): ما هي الاسس المعتمدة في تصنيف التهديدات.

س (3): عرف التهديدات الطبيعية.

س (4): يترتب على التهديدات الطبيعية لأمن المعلومات العديد من الأضرار، عددها.

س (5): عرف التهديدات البشرية لأمن المعلومات.

س (6): ما المقصود بالتهديدات البشرية من داخل المنظمة، ولماذا تحصل؟

س (7): وضح من خلال الشكل الأسباب الفعلية للتهديد البشري من داخل المنظمة.

س (8): ضع دائرة أمام الاجابة المناسبة.

المهاجمون من داخل المنظمة هم:

A- طالبي الوظائف الجدد	B- الموظفون الحاليون المستمرين في العمل
C- الموظفون السابقون الذين غادروا المنظمة	D- (B + C)

س (**9**): وضح من خلال الجدول نماذج من التهديدات الداخلية لأمن المعلومات.

س (**10**): وضح من خلال الشكل خريطة التهديدات الداخلية لأمن المعلومات.

س (**11**): هناك إجماع من قبل المتخصصين على أن الاخطاء التقنية تشكل الحصة الأكبر من بين أسوأ الأخطاء التي يرتكبها المستخدمون لنظم المعلومات، علق على هذه العبارة.

س (**12**): عرف التهديدات الخارجية مبيناً أهم البواعث لهذه التهديدات.

س (**13**): من وجهة نظرك، من الذي يسرق المعلومات، وما هي أكثر أنواع المعلومات المستهدفة؟

س (**14**): وضح من خلال الشكل الطرق الأربعة الرئيسة لسرقة المعلومات.

س (**15**): ما المقصود بالتجسس الصناعي أو التنافسي، وما هي أشكاله؟

س (**16**): يؤكد الخبراء على أن التجسس الصناعي في إزدياد مستمر، يا ترى ما هي اسباب ذلك؟

س (17): تعد السرقة والتخريب من قبل الموظفين خرقاً مقصوداً لأمن المعلومات، كيف، وما هي أشكالها؟

س (18): يعد التعرض العرضي للمعلومات من قبل الموظفين التهديد الأكثر شيوعا، كيف ولماذ يحصل؟

س (19): وضح من خلال الشكل أهم مجالات إختراق أمن المعلومات.

س (20): يمكن اختراق أمن الملفات الورقية من خلال العديد من الجوانب، بينها باختصار.

س (21): يمكن إختراق أمن المعلومات من خلال أجهزة الفاكس والهاتف المحمول، كيف؟

س (22): تمثل الثرثرة أحيانا فرصة لختراق أمن المعلومات، فسر ذلك.

س (23): يأخذ التجسس وإنتحال الصفة بوصفها مجالاً لاختراق أمن المعلومات عدة أشكال، ما هي؟

س (24): ضع دائرة أمام الاجابة المناسبة

ترتكز الفرص الخاصة بختراق أمن المعلومات من خلال التجسس وإنتحال الصفة على:

A- إغـــراء الموظـــف بالمـــال والامتيازات	B- إكراه الموظف وإجباره
C- خلـــق الطمأنينـــة في نفـــس الموظف للتحدث	D- جميع ما ذكر صحيح

س (25): وضح من خلال الشكل أهم نقاط الضعف التي قد تؤدي إلى الإخلال بأمن المعلوماتز

س (26): حاكمية أمن المعلومات في كثير من الاحيان أقل من ناجة لوجود عدد من نقاط الضعف، ماهي؟

س (27): تتدرج نقاط ضعف الفراد العاملين ضمن أربع فئات، وضح من خلال الشكل هذه الفئات.

س (28): ما علاقة نقص المعرفة /الوعي والتدريب بأمن المعلومات؟

س (29): يشير المتخصصون الى أن الفراد غير معصومين من وقوع حادث أمني بسبب الخطأ البشري، علق عل العبارة.

س (30): نقص مشاركة الأفراد العاملين هو نقطة الضعف التي يصعب التعامل معها، كيف؟

س (31): ما المقصود بنموذج نضج القدرة وما هي أهم مستوياته؟

س (32): في حين أن مبادئ إدارة العملية بسيطة بما فيه الكفاية لفهمها وإدراكها، إلا ان مستويات النضج العلى لهذه العمليات يصعب تحقيقها، لماذا؟ علل.

س (33): وضح طبيعة العلاقة بين العمليات التي يملكها مقدمي الخدمات ونقاط الضعف في أمن المعلومات.

س (34): ما هي أهم المجالات التي يملكها مصممي النظام والمنفذين؟

س (35): تعد غدارة الهوية والوصول الى المعلومات أمراً أساسياً لحماية أمن المعلومات، كيف؟

س (36): تقع العمليات التي لها صلة بإدارة البيانات في ثلاث فئات رئيسة، حددها.

س (37): العمليات التي يملكها المستخدمون تقع تحت شعار" احضر جهازك الخاص بك إلى بيئة العمل"، علق على العبارة.

س (38): إن الفشل في تكنولوجيا المعلومات نادراً ما يكون تدريجياً، كيف؟

س (39): من وجهة نظرك، هل تعد صناعة تكنولوجيا المعلومات والاتصالات من الصناعات الآمنة، أم لا.

س (40): وضح من خلال الشكل العواقب غير المقصودة لصناعة تكنولوجيا المعلومات والاتصالات قدر تعلق الأمر بأمن المعلومات.

س (41): اذكر مثالاً واحداً لكل من أنواع العواقب غير المقصودة لتكنولوجيا المعلومات والاتصالات والتي لها علاقة بأمن المعلومات.

س (42): أجب بوضع إشارة (صح) أو إشارة (خطأ) أمام العبارات الآتية:

	العبارات	الاشارة
1	التهديدات الطبيعية تتصف بأنها تكون شاملة وكبيرة الأثر على أمن المعلومات	

2	إذا تم فقد الاتصال بالإنترنت لأي سبب من الأسباب مثل الهجمات على خطوط الشبكة فإن جميع الخدمات المقدمة من خلال السحب تكون متوفرة حتى ولم لم يتم إصلاح الانقطاع.	
3	استخدام النظم الحاسبية أسهمت في التخلص من الملفات الورقية التي كانت تستحوذ على النسبة الأكبر من الملفات المستخدمة في أغلب المنظمات.	

الفصل الخامس

الأسباب الأخرى لانعدام أمن المعلومات

5

- تمهيد
- أولاً: الأسباب (العوامل) الداخلية للمنظمة
- ثانياً: الأسباب (العوامل) الخارجية . . المشهد المتغيّر باستمرار
- ثالثاً: أمن المعلومات يجب أن لا يمنع التفكير الابتكاري

الفصل الخامس

الأسباب الأخرى لانعدام أمن المعلومات

Other drivers of information security

تمهيد:

يناقش هذا الفصل العوامل الأخرى التي ينبغي على الإدارة الاهتمام بها ، والتي تسهم في انعدام الأمن للمعلومات و تكون مصدر قلق للإدارة.

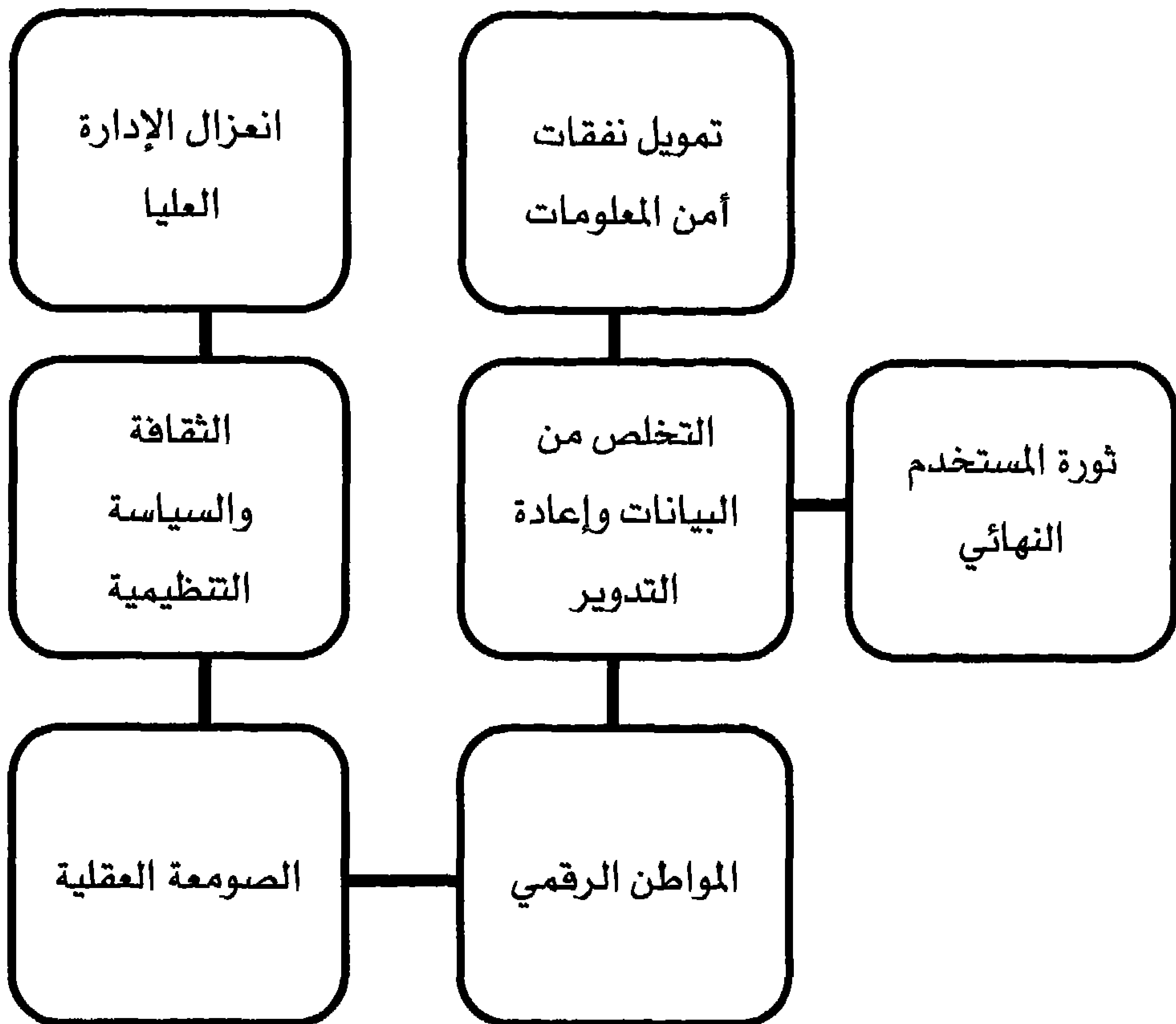
المديرون الجيدون يسعون لإزالة العقبات، وتوفير المساعدة والاعتراف بالجهد

حيث تعد مهمة الحفاظ الجيد بما فيه الكفاية على أمن المعلومات في المؤسسة مهمة معقدة للغاية. ويعتقد كثيرون أن أي شخص بإمكانه أن يفعل هذا دون أن يتحمل أية مسؤولية لذلك. وفي هذا الفصل نتناول الموضوعات التي لا تغطيها المعايير أو المبادئ التوجيهية أو الممارسات الجيدة والتي لا يمكن العثور عليها (إذا كانت مدركة ومعترف بها) في كل مكان. عندما تظل غير مدركة (معترف بها) و/ أو لا أحد مسؤول عنها ، فإن هذه الموضوعات يتم إضافتها إلى انعدام أمن المعلومات في المنظمة. والسؤال الذي يطرح نفسه هنا هو ما هي أسباب القلق حول أمن المعلومات (Causes for concern)؟ للاجابة عن هذا السؤال يشير المتخصصون إلى أن هناك العديد من الاسباب التي تقود إلى حدوث القلق بخصوص فقدان أمن المعلومات في المؤسسة، ويصنف الكتاب هذه الاسباب بشكل عام إلى نوعين هما:

أولاً: الأسباب (العوامل) الداخلية للمنظمة

Internal to the organization

تقع هذه الاسباب داخل حدود المنظمة والتي يمكن للادارة التحكم بها بقدر أو آخر، والشكل الآتي يوضح هذه الاسباب (العوامل):



الشكل (5 ـ 1)

الاسباب الداخلية للقلق حول أمن المعلومات

1- انعزال الادارة العليا:

الحكم الرشيد يتطلب الالتزام والدعم من الادارة الأعلى. وبدون ذلك فإن الناس ليس لديهم خيار سوى تخمين ما هو متوقع منهم، وتقديم أفضل جهد ممكن لانجاز الامور في ضوء توقعاتهم لما هو مطلوب منهم إنجازه. في أعلى المستويات من الهرم في أي منظمة، يتم حتماً تخفيف المعرفة التفصيلية التي يفترض ايصالها اليها وفي ذات الوقت تكون الضغوط والمطالب عليها كبيرة على النحو الذي ينعكس على الوقت المتاح لديها للتعامل مع هذه المطالب. عليه فإن الحصول على انتباهها يتطلب مهارات الاتصال الجيدة، وهي قضية عمل واضحة والقدرة على ايصال الرسالة في وقت قصير.

2- الثقافة والسياسة التنظيمية:

حقيقة من حقائق الحياة هي أنه لكي تلعب لعبة معينة فإن الامر يتطلب معرفة من لديه نفوذ في المنظمة ومعرفة كيفية فتح حوار هادف معه. عليه فإن الفشل في القيام بذلك سوف يقود إلى تحييد الجهود الجبارة التي يبذلها أؤلئك الذين يتمثل دورهم في تعزيز الأمن.

3- الصومعة العقلية:

ضعف التعاون بين الوظائف حالة مألوفة في المنظمات المسيسة. عندما تكون هذه هي الحالة السائدة، فإنه يمكن فقط للقيادة التحويلية تغيير الوضع الراهن. ويعد تحقيق مثل هذا التغيير أصعب في المنظمات الكبيرة بالمقارنة مع المنظمات الأصغر. ومن وجهة نظر أمن المعلومات هذا يعني شيئاً واحدا: ألا وهو " المشكلة".

4- المواطن الرقمي:

المقالات التي نشرت في عام (2001) قدمت مفهوم "المواطن الرقمي" و "المهاجر الرقمي". المواطن الرقمي يعني الجيل الذي أتيحت له الفرصة للتفاعل مع التقنيات الرقمية في سن مبكرة، واصبح لديه معرفة تامة بمفاهيمها. المواطن الرقمي قاد ثورة المستخدم النهائي التي سيتم مناقشتها لاحقاً. المهاجر الرقمي ما زال يحتفظ بالعديد من العناصر التي كانت مستخدمة ما قبل الحقبة الرقمية ويستخدم العالم الرقمي بجهد اكبر، هؤلاء هم الناس الذين يجب ان يقوموا بقراءة الكتيبات الخاصة بطريقة الإستخدام.

5- التخلص من البيانات وإعادة التدوير:

القضية الاخرى للحوكمة تتعلق بالاحتفاظ والتخلص من البيانات للتأكد من أن الأجهزة تم تنظيفها كلياً مما تحتوي من بيانات المنظمة. فإنه من الحكمة إشراك المستشار القانوني قبل اتخاذ أي إجراء ومن ثم اتخاذ الخطوات المناسبة لمحو كافة البيانات من هذه الأجهزة.

6- تمويل نفقات أمن المعلومات:

Funding information security expenditures

يعد تمويل أمن المعلومات جزءاً من الحاكمية. ويمكن أن تؤدي السياسة التنظيمية (Executive detachment) إلى جعل هذا الموضوع مثيراً للجدل. هناك أولئك الذين يقولون إن حماية معلومات المنظمة يتطلب استثمارات. هذا يقودنا إلى السؤال "ما هو العائد على الاستثمارات في أمن المعلومات؟" يرى آخرون بأن تمويل أمن المعلومات هو جزء من تكلفة ممارسة الأعمال المنظمية وأن مثل هذه النفقات يجب أن تكون بمحاذاة قيمة

الأصول/ الموجودات المطلوب حمايتها، بنفس الطريقة التي تدفع بها أقساط التأمين. كل الحجج صالحة وتستمر المناقشة فيها ويبقى الجدل شبه الفلسفي طالما القضية لم تحل. ويغطي تمويل أمن المعلومات الأنشطة في أنحاء مختلفة من المنظمة مثل:

- المشتريات الفنية لمقدم خدمة تكنولوجيا المعلومات (إذا كانت داخلية) والمشتريات المتنوعة عبر منظمة (مثل المنتجات المضادة للفيروسات، ورموز لمصادقة المستخدمين النهائيين، وتحديث المعدات والبرمجيات وصيانتها، ...إلخ).
- تقديم خدمات استشارية وتدقيقية لتحديث استراتيجية أمن المعلومات وسياستها، تحليلات تأثير الأعمال وتقييم المخاطر.
- مواد التدريب والتوعية، فضلا عن ورش العمل والشهادات.
- توفير الموارد لبرنامج تصنيف البيانات المستمرة.
- ضمان إنجاز عمليات التخلص من البيانات من دون الاضرار ببيانات المنظمة.

إن فصل هذه الأنشطة المخصصة تحديدا لأمن تكنولوجيا المعلومات عن الأنشطة التشغيلية الأخرى ليست سهلة. ورغم ذلك، الأدلة المنشورة تشير إلى أنه نفقات تكنولوجيا المعلومات عادة ما تكون في حدود (3 ـ 5٪) من مجموع النفقات الكلية للمنظمة، ويمثل أمن المعلومات حوالي 5٪ من هذه النفقات.

ويظهر التقرير(5) لمجموعة (Gartner) للعام (2012) أن متوسط الإنفاق لكل موظف في السنة في الولايات المتحدة كان (13.600$) لمدة

سنة من العمل (220 يوما)، ومعدل النفقات لكل موظف يعمل في تكنولوجيا المعلومات يوميا هو (62$)، منها حوالي (3 دولار) لأمن المعلومات. وهذا المبلغ هو مماثل لسعر فنجان من القهوة. الضغط المستمر للحد من النفقات يتطلب في كثير من الأحيان تقديم التبريرات المالية للأشياء التي يتعذر قياسها كميا بسهولة، مثل العائد على الاستثمار (ROI) على البيانات أو المحافظة على السمعة. الجزء الخاص بالإنفاق في معادلة تحليل العائد على الاستثمار لأمن المعلومات واضح ومباشر. إذ يدرك الممارسون من ذوي الخبرة أن بعض البنود يمكن أن تترك بأمان خارج الحسابات، على سبيل المثال تكلفة الشراء، ورسوم الصيانة وتكاليف التركيب. أما الجزء الخاص بالفوائد (المنافع) من المعادلة فإنه يشبه العمل من وحي الخيال الذي يكون فيه من السهل نسبيا التوصل إلى أرقام "جيدة". الخطر هو في المستقبل، والبيانات لدعم تنبؤات موثوق بها ليست متاحة. وهذا يعني أن أية أرقام يتم عرضها عن الفوائد لا يمكن التحقق من صحتها، ومن ثم لا تكون مضمونة. هذه الأرقام هي مشروطة (ضمنياً) بالعديد من الافتراضات مثل: أن المنتج سيعمل كما وعد البائع، إذا تم تثبيته بشكل صحيح. هذه ليست الحال دائماً.

وهناك أيضا خطر ضمني وهو أن السعي لتحقيق وفورات في التكاليف يمكن أن يؤدي إلى ما يصطلح عليه "فقدان شهية الميزانية Budgetary Anorexia " (أو توفير المال بغض النظر عن التكلفة (SMRC)) الذي قد يقود في نهاية المطاف إلى نتائج عكسية. التطبيقات النموذجية لـ (SMRC) تشمل:

- الموافقات مع التركيز على خفض التكاليف.
- تأجيل النفقات كما في حالة: "من المؤكد أن هذا يمكن أن ينتظر سنة أخرى".
- تأجيل التوظيف كما في حالة: "العمل أكثر ذكاء، وليس أصعب"
- الفصل بين الواجبات محدودة أو معدومة.
- الباب مفتوح للتغيرات غير الصحيحة أو غير المجربة.
- الأجر الجامد مما يؤدي إلى عدم القدرة على توظيف المواهب المطلوبة والاحتفاظ بهم.

عندما تستخدم كل هذه الحالات باستمرار، فمن المحتمل جدا أن الموظفين ذوي الخبرة سوف يبحثون عن وظيفة في مكان آخر ويعثرون عليها طالما أن هنا نقص في الخبرات من الأفراد العاملين.

7- ثورة المستخدم النهائي The end user revolution:

إن مفهوم المواطن الرقمي قادنا إلى الابتكارات الحديثة بحماس كبير، إلى حد الاصطفاف بين عشية وضحاها خارج متجر لشراء أحدث الإبتكارات. يعتبر هذا الإجراء مقبول في مجالهم الخاص بهم كأفراد أحرار في فعل ما يحلو لهم و / أو يمكن تحمله. هذه الأجهزة متواجدة بكثرة في بيئة الشركات، كما ان الأفراد يشعرون بانهم مخولون لتحدي معايير الشركات ويصرون على أن يتم السماح لهم باستخدام أجهزتهم أوالتطبيقات الخدمية الخاصة بهم.

وقد أدى هذا إلى مفهوم (إحضار جهازك الخاص (BYOD))، وتقوم المنظمات بالمكافحة من أجل فهم وإدارة الآثار الأمنية المترتبة على هذا. مع

استمرار مفهوم BYOD بالتوسع، يبدو أن ما وصلنا اليه أصبح لا رجعة فيه. هذا يعني أن الناس يمكنهم الوصول وتحميل وتخزين بيانات الشركات الحساسة عن طريق جهاز خارج الهيكل الأمني للمنظمة. ما هو أكثر من ذلك، قد يحتوي مثل هذا الجهاز على تطبيقات غير معروفة للمنظمة. هذه التطبيقات المجانية أو المنخفضة التكاليف، والمصممة من قبل اشخاص مجهولين وبدون شهادة أمان، قد تشمل على البرامج الضارة جداً. إضافة إلى الألم الذي قد تسببه، ويمكن الاطلاع على بيانات الشركات من أي مكان، على سبيل المثال كوفي شوب يقدم "خدمة الإنترنت مجاناً" بدون عملية تشفير قد تسمح لطرف ثالث بالحصول على البيانات.

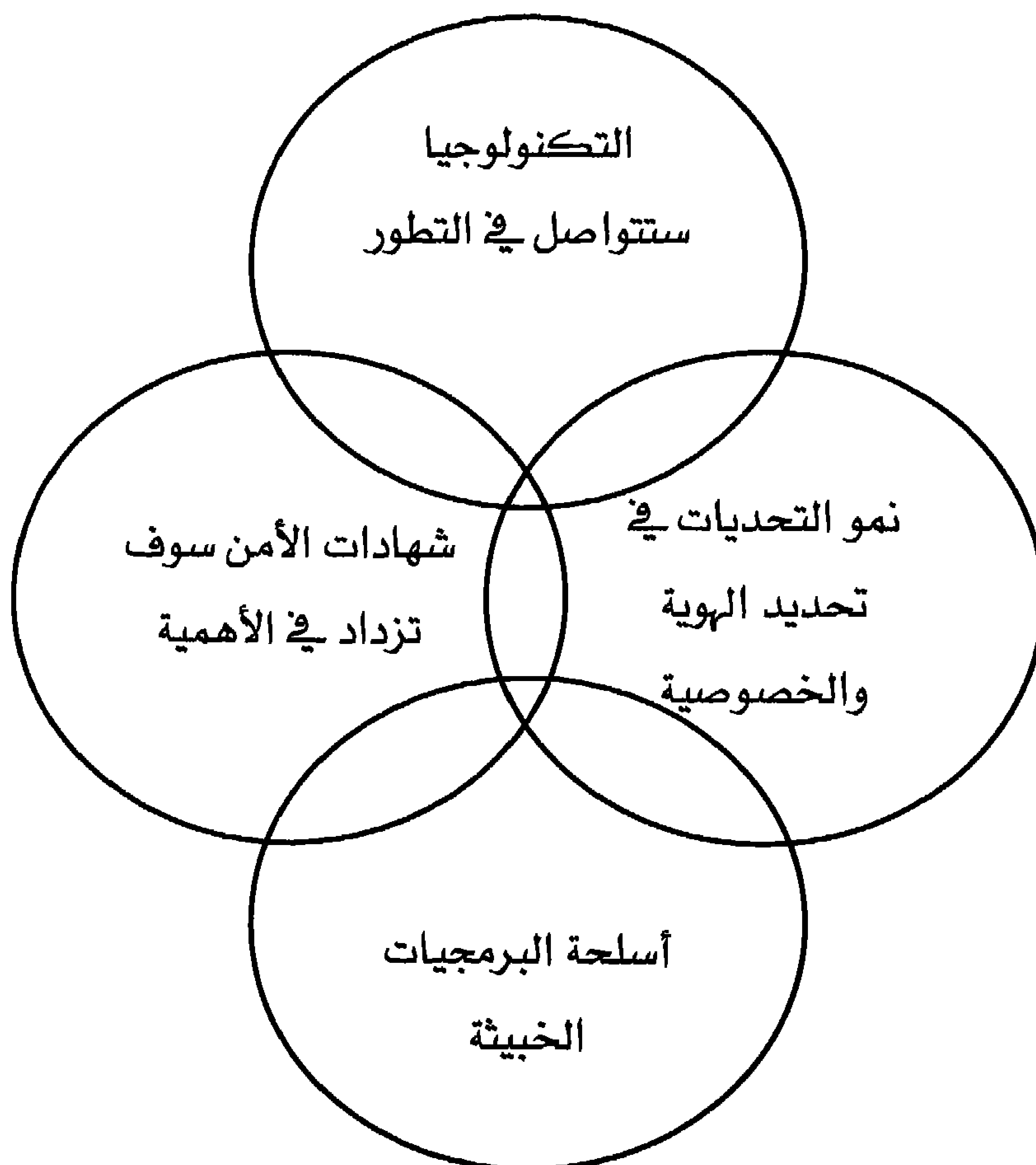
في الطرف الآخر تشجع التدابير الأمنية المشددة (digital natives) لتجاوز القيود المفروضة على المنظمة عن طريق نسخ المعلومات الحساسة إلى حساباتهم في السحابة (Cloud) حيث ستكون دون وقاية. وهذا يجعل عمل القرصان أسهل بكثير... وتشمل المخاطر الجديدة الأخرى التي يتم إيجادها بوساطة (digital natives) استخدام الشبكات الاجتماعية لتبادل المعلومات الحساسة مع أقرانهم. إظهار (digital natives) مستوى أكبر بكثير من الثقة في الناس الذين يقابلونهم عبر الإنترنت من (digital immigrants).

ثانياً: الأسباب (العوامل) الخارجية.. المشهد المتغير باستمرار

External factors: the constantly changing landscape

لا توجد أي إشارة أو سبب للاعتقاد بأن معدل الابتكار في نظم المعلومات والتكنولوجيا سوف يبطئ أو يتعرقل في المستقبل المنظور، إلى

جانب نمو التحديات في تحديد الهوية والخصوصية، وتنوع أسلحة البرمجيات الخبيثة، وتزايد أهمية الشهادات في أمن المعلومات، والشكل (5 ـ 2) يوضح هذه الأسباب.



الشكل (5 ـ 2)

الاسباب الخارجية للقلق حول أمن المعلومات

1- التكنولوجيا ستتواصل في التطور:

Technology will continue to evolve

يمكن توقع أن الأجهزة سوف تكون أسرع وأصغر حجما وأخف وزنا مع بطارية ذات حياة أطول والشاشة ستعمل باللمس. ودورة حياتها من الشراء إلى التقادم سوف تتواصل إلى أن تكون قصيرة على نحو متزايد، سوف تحتوي الأجهزة على التكنولوجيات الجديدة وتكون متصلة بالإنترنت. كثيرة هي بالفعل ـ في المصاعد، وأنظمة تكييف الهواء، وآلات البيع، وغيرها، يمكن أن تصبح أهدافا للتعطيل. وتشمل وعود المستقبل السيارات والنظم الروبوتية الجراحية.

الأفراد المبدعون سيوفرون خدمات جديدة على الإنترنت ـ حيث كان ما يسمى الويب (2.0) مفاجأة لمعظم الناس والخدمات مثل المدونات، وتبادل الصوت والفيديو، والألعاب متعددة اللاعبين، والشبكات الاجتماعية، المزادات على الانترنت وغيرها الكثير يمكن أن تستكمل لتوفر عروضاً جديدة لا يمكن تصورها حاليا.

2- نمو التحديات في تحديد الهوية والخصوصية:

Growing challenges in identity and privacy

الناس بوصفهم كائنات حية اجتماعية، يرغبون ويحتاجون إلى التفاعل مع بعضهم البعض بطريقة تسمح بقدر من السيطرة والتحكم. في الفضاء الإلكتروني من المهم أن تكون قادراً على الثقة بهوية الأفراد لمنع الغش وتعزيز الأمن القومي. تحتاج إدارات المنظمات لضمان أن الأفراد الذين تتعامل معهم هم نفسهم الذين يقولون انهم هم، وأن يكونوا مرخصا لأن

يفعلوا ما يفعلونه حقاً. يريد الأفراد أن يكونوا محل الثقة (الوثوق بهم) ويحتاجون إلى ثقة المنظمات التي يتفاعلون معها لحماية المعلومات الشخصية. بالإضافة إلى كلمات السر (شيء ما تعرفه)، يستخدم العديد من المنظمات الآن تقنيات إضافية للتصديق الفردي مثل البطاقات أو الرموز (شيء ما لديك) تستخدم كعامل ثان لتحديد الهوية. في النهاية هناك الأجهزة التي تفحص البصمة أو قزحية العين (شيء ما فيك أنت).

3- **أسلحة البرمجيات الخبيثة** Weapons grade malware:

يمكن القول أنه منذ ذلك الحين الذي أصبحت فيه البرمجية الضارة (Stuxnet) معروفة لدى الجمهور في عام (2010)، ظهرت هناك مخاوف من انه يجسد الدليل على أن الهجمات المستهدفة يمكن إطلاقها ضد أي شخص، وأنه فتح الباب أمام عسكرة الفضاء الإلكتروني. اثنين من المقالات التي نشرت في مجلة (الإيكونوميست Economist)، وآخرها في نهاية شهر آذار من عام (2013)، بعنوان "تجارة الأسلحة الرقمية Digital Arms Trade" ومقالة سابقة في نيسان (2008)، بعنوان "أمن الحاسبة: ألم في الجسم Computer Security: Pain in the body " ناقشتا برمجيات الجريمة كخدمة، وتم تسليط الضوء على وجود سوق لأدوات صممت بخبرة للهجوم على البرمجيات. والتقارير تشير إلى مقدار الإيرادات المتحققة عن بيع بعض من هذه الادوات رغم أنها بالمقارنة مع المعدات العسكرية، تعد صغيرة. والسؤال الذي يطرح نفسه هو: هل سيصبح الفضاء الإلكتروني ميدان جديد في المعركة؟ الاجابة ربما.

4- شهادات الأمن سوف تزداد في الأهمية:

Security certifications will increase in importance

كما ذكرنا في وقت سابق، فإن أمن المعلومات ليس مهنة مقننة، بل هو مهنة غير محكمة (غير منضبطة)، وبالتالي لا يوجد أي متطلب من أي شكل من أشكال الشهادة. وبينما يعد أمن المعلومات أمراً بالغ الأهمية، على النحو الذي يبرر طلب مثل هذه الشهادات، إلا أن الشهادات المهنية في مجال أمن المعلومات تتصف بأنها اختيارية بالنسبة للأفراد، ولكن قد يشترط بعض أرباب العمل وإدارات المؤسسات حصول الأفراد المتقدمين لشغل إحدى وظائف أمن المعلومات لديها بوصفها شرطاً من شروط التوظيف، فمن المرجح هنا أنه كلما قدرت الإدارة العليا أهمية أمن المعلومات، فسوف يكون هناك اتجاه نحو إعتبار مثل هذه الشهادات كشرط ومتطلب للتوظيف. العديد من الهيئات تقدم شهادة الامتثال إما مع معيار أو مجموعة من الممارسات الجيدة في حين أن آخرين تصدر شهادات تثبت المعارف والخبرات لدى الأفراد في مجالات محددة من أمن المعلومات. وتتدرج هذه الشهادات في ثلاث فئات هي : التنظيمية والمهنية والشخصية. وتشمل الشهادات التنظيمية، على سبيل المثال، الامتثال لـ (ISO 27001) "نظام إدارة أمن المعلومات" و قانون إدارة أمن المعلومات الفيدرالي في الولايات المتحدة (FISMA). البعض منها قد يكون اختياري (ISO 27001)، في حين أن البعض الآخر قد يكون إلزاميا في مجالات محددة من النشاط مثل معيار أمن البيانات لصناعة بطاقات الدفع (PCI-DSS). وهناك العديد من الشهادات، مثل تلك التي تمنح من قبل جمعية

الرقابة والتدقيق لنظم المعلومات (Information Systems Audit and Control Association (ISACA)) ومن نماذج هذه الشهادات نذكر:

- شهادة مدقق أمن المعلومات (CISA: Certified Information Security Auditor).
- شهادة مدير أمن المعلومات (CISM: Certified Information Security Manager).
- شهادة في المخاطر ورقابة نظام المعلومات (CRISC: Risk and Information System Control). هناك أيضا الشهادات التي تمنح من قبل الاتحاد الدولي لأمن نظم المعلومات (ISC2)، وتشتمل على:
  - الشهادة المهنية لأمن نظم المعلومات (CISSP: Certified Information Systems Security Professional).
  - الشهادة المهنية في أمن دورة حياة البرمجيات وغيرها من الشهادات.

بالإضافة إلى ذلك، فإن الباعة وشركات التدريب تقدم أيضا شهادات مختلفة. والفئة الثالثة من الشهادات هي معادلة لرخصة القيادة وتتطلب من الأفراد إكمال برنامج التدريب أو التوعية واجتياز الاختبار. وقد وضعت تلك الشهادات وتم اختبارها على مدى سنوات عديدة من قبل العديد من المنظمات. ومن الأمثلة على تلك الشهادات، شهادة أمن الميدان التي تطلبها الأمم المتحدة من أولئك الذين يسافرون إلى موقع العمل الميداني المخصص لأداء المهام الموكلة لهم من قبل الهيئة. وهذه الشهادة الخاصة صالحة لمدة ثلاثة سنوات بعد إستكمال الاختبار.

ثالثاً: أمن المعلومات يجب أن لا يمنع التفكير الابتكاري

Information security should not inhibit innovative thinking

فتحت التكنولوجيات المبتكرة (كما تمت الاشارة اليها في الفصل السابق) فرصاً وجلبت معها آثار جانبية غير معروفة ونتائج غير متوقعة. العيش مع عدم اليقين والمخاطر أمر لا مفر منه والتحدي الإداري هو أحد جوانب فهم قدرتها على إدارة التغيير المترتب على التكنولوجيا. ولحماية المنظمة، يميل رئيس ضباط أمن المعلومات إلى أن يكون حذراً، وغالبا ما يشار إليه باسم "الدكتور لا Dr. No". هذا يعمل بشكل جيد في المنظمات التي تنفر من المخاطر حيث يعد التقاعس التكنولوجي حكمة في التصرف ولكن يمكن أن يكون محبطا للقوى العاملة عندما تكون التكنولوجيات الشخصية هي أكثر تقدما من تلك الموجودة في بيئة الشركات.

في الطرف الآخر، تلك الإدارة التي لديها شهية أكبر للخطر والريادة في تبني التكنولوجيات المبتكرة يمكن أن توفر الأرضية لاغتنام الفرص لتطوير خدمات الأعمال والتوصل إلى الحلول قبل الآخرين والاستفادة وفقا لذلك. ينبغي للإدارة الادراك منذ البداية أن التقدم على الآخرين يعني التعلم من الخبرة حول الآثار الجانبية والعواقب غير المقصودة. يتناول الفصل التالي أن التحديات لقياس ما يمكن أن يكون لا تقدر ولا تحصى.

أسئلة الفصل

س (1): وضح من خلال الشكل الاسباب الداخلية للقلق حول أمن المعلومات.

س (2): كيف يسهم إنعزال الادارة العليا في إثارة القلق تجاه أمن المعلومات؟

س (3): ضعف التعاون بين الوظائف حالة مألوفة في المنظمات المسيسة، علق على العبارة مبيناً كيفية تشكل الصومعة العقلية.

س (4): ما المقصود بمفهوم المواطن الرقمي" و "المهاجر الرقمي"؟

س (5): يعد تمويل أمن المعلومات جزءاً من الحاكمية. ويمكن أن تؤدي (Executive detachment) السياسة التنظيمية إلى جعل هذا الموضوع مثيراً للجدل، برأيك ما هي نقاط الخلاف التي تثير مثل هذا الجدل؟

س (6): ما المقصود بمصطلح "فقدان شهية الميزانية Budgetary Anorexia"، أذكر نماذج من تطبيقاته.

س (7): لقد أدت ثورة المستخدم النهائي إلى تكريس ظاهرة " إحضار جهازك الخاص" المعروف إختصاراً (BYOD)، التي ترتبت عليها آثاراً غير مرغوبة على أمن معلومات المؤسسة، كيف؟

س (8): وضح من خلال الشكل الاسباب الخارجية للقلق حول أمن المعلومات

س (9): من وجهة نظرك هل هناك سقف لتوقعات تطور تكنولوجيا المعلومات والاتصالات؟

س (10): بوصفك متخصصاً في أمن المعلومات ماذا تقترح على إدارات المنظمات للتعامل مع ظاهرة نمو التحديات في تحديد الهوية والخصوصية.

س (11): فتحت اسلحة البرمجيات الخبيثة الباب أمام عسكرة الفضاء الإلكتروني، كيف؟

س (12): يشير المتخصصون إلى أن أمن المعلومات ليس مهنة مقننة، بل هو مهنة غير محكمة (غير منضبطة)، علق على هذه العبارة موضحاً مستقبل الحاصلين على شهادة أمن المعلومات.

س (13): من وجهة نظرك هل يجب أن يمنع أمن المعلومات التفكير الابتكاري، لماذا؟

الفصل السادس

قياس أمن المعلومات

6 

- تمهيد
- أولاً: كيفية قياس أمن المعلومات
- ثانياً: إعداد التقرير عن مقاييس أمن المعلومات

الفصل السادس

قياس أمن المعلومات

Measuring Information security

تمهيد:

في هذا الفصل سوف يتم توضيح مدى إمكانيات وضع الأرقام على الموضوع الذي من الصعب قياسه:

- مقاييس الأمن. هل يمكن قياس الأمن، وإذا كان الأمر كذلك، كيف؟
- ماذا ينبغي الإبلاغ عنه، متى، وإلى من وكيف؟

أولاً: كيفية قياس أمن المعلومات Measuring Information Security

لن يكون جيداً إذا كانت مؤسستك تقول "كان لدينا مستوى الأمن الشهر الماضي (82.5٪)"؟ لسوء الحظ، هذا الأمر غير ممكنا ويمثل تحديا لأنه لا توجد طريقة بسيطة للتعبير بالأرقام في مفهوم معقد مثل الأمن. وينطبق الشيء نفسه على أشياء أخرى كثيرة، مثل الألم والحب ... وربما لهذا السبب أشار مكتب (Albert Einstein) في (Princeton) قائلا: "ليس كل ما يهم يمكن عده. ليس كل ما يمكن عده يكون مهماً".

هل يمكنك أن تقول كيف هو أمن المعلومات الخاص بك الآن؟ كيف ينبغي أن يكون؟ أو ما ذا عن القدرة على القول بأنه: "كان مستوى أمننا في الشهر الماضي أفضل مما كانت عليه في هذا الوقت من العام الماضي". قد

نكـون قـادرين علـى تقـديم مفـاهيم مثـل "أفـضل" أو "أسـوأ" لمـا تم تعريفـه بوضـوح، وأصـبحت مفهومـة ومتفـق عليهـا. ولكـن هـذا لا يعـني أن الوضـع ميؤوس منه. ولحل هذه الاشكالية يقترح هـذا الفصل إعتماد نهج واقعـي هـو إستخدام مؤشرات الخطر.

لا يمكنك إدارة ما لا تستطيع قياسه **You cannot manage what you do not measure**

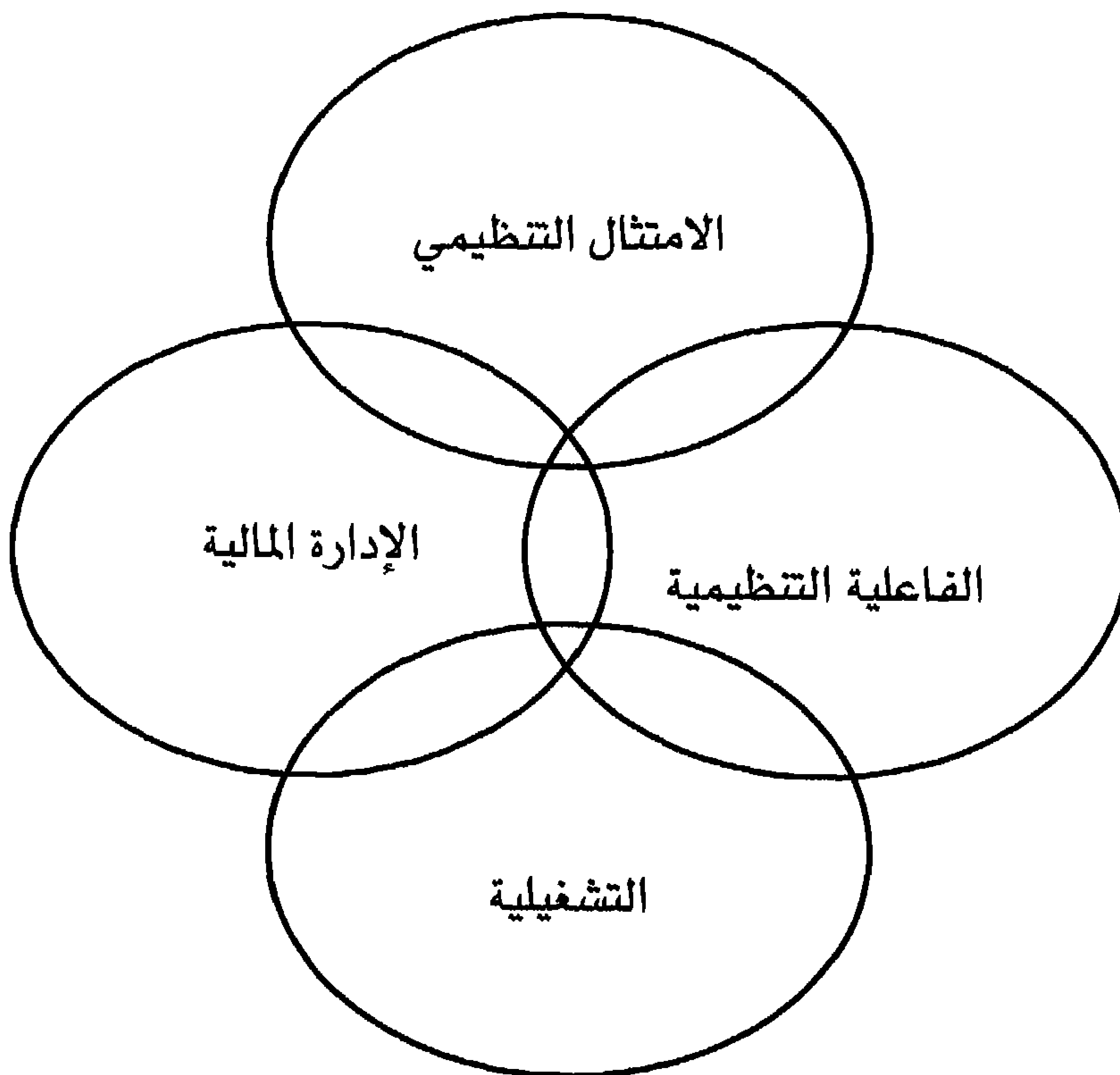
في عام 1893 ، قال وليام طومسون (اللورد كلفن): "إذا كنت تستطيع قياس الموضوع الذي تحدثت عنه، ويمكنك التعبير عن ذلك من خلال عدد (رقم محدد)، فأنت تعرف شيئاً عن الموضوع الخاص بك، ولكن إذا كنت لا تستطيع قياسه، فإن معرفتك ضعيفة وغير مرضية. وهـذا الوصف ينطبق أحيانا على المعلومات التي لا يمكن قياسها و/أو تكون مقاييسها غير متاحة. هناك كميات هائلة من المعلومات المتعلقة بالأمن التي يمكن جمعها. كما أن هناك العديد من المصادرالتي أدرجت مقاييس أمن المعلومات الممكنة (على سبيل المثال COBIT لأمن المعلومات). وهذه المقاييس تركز على جمع المعلومات، تحليلها والإبلاغ عنها من خلال الأساليب المتاحة، ولكن هذا لا يضمن أن كل هذه المقاييس سوف تكون مفيدة لمنظمة معينة. معرفة ما يجب قياسه، وكيفية القيام بذلك وكيفية التواصل, تؤدي إلى نتائج يمكن أن تساعد على تحسين كفاءة الأمن وفعاليتها وسمعة المؤسسة المعنية.

1- لماذا يجب امتلاك المقاييس الأمنية:

Why it makes sense to have security metrics

هناك العديد من الأسباب الوجيهة لبذل الجهد لامتلاك مجموعة من المقاييس الأمنية. ولعل الأكثر أهمية هو أنه في حالة عدم وجود مقاييس تعتمد

المنظمة على ما يعرف إختصاراً (FUD) أي الخوف وعدم اليقين والشك (Fear, Uncertainty and Doubt)، وكما قال (Lord Kelvin)، معرفتك ضعيفة وغير مرضية. وبشكل أكثر تحديدا، هناك أربعة مجالات لتجسيد اهمية المقاييس ذات الصلة، بل ضرورتها وهي كما مبينة في الشكل (6 ـ 1):



الشكل (6 ـ 1)

مجالات تجسيد أهمية قياس أمن المعلومات

- **الامتثال التنظيمي:** قد تؤدي حوادث أمن المعلومات إلى فشل المنظمة في تلبية الشروط والمتطلبات التي وضعتها التشريعات. قد تكون هذه التبعات قانونية ومالية والسمعة. ويمكن وضع مقاييس لحادث

أمني في سياق توفير معلومات واقعية تثبت أن العناية الواجبة المناسبة تمت ممارستها.

- الإدارة المالية: هناك حاجة بانتظام إلى استثمارات في مختلف جوانب أمن المعلومات والمقاييس تثبت أن الاستثمارات الماضية في أمن المعلومات كان لها ما يبررها.
- الفاعلية التنظيمية: يمكن أيضا أن تستخدم القياسات لتثبت لأصحاب المصلحة في المنظمة فاعلية برنامج أمن المعلومات.
- التشغيلية: هي الاهتمام الرئيسي لمدير دائرة نظم المعلومات مسؤول النظم ومسؤولوا البيانات. وهناك العديد من هذه المقاييس ولكن ذات قيمة محدودة لمديري الأعمال.

2- القياس المفيد وخصائصه What makes a metric useful:

مقاييس الأمن مفيدة بشكل خاص عندما توفر الإنذار المبكر عن المناطق الساخنة المحتملة أمنيا. وتسمى هذه المقاييس "المؤشرات الرئيسية Leading indicators". مقياس الأمن هو بالتأكيد ليس مفيداً عندما تكون الاستجابة من أولئك الذين يتم إبلاغهم عنها هو "ماذا في ذلك؟

لتجنب الرد "ماذا في ذلك"، ينبغي أن يكون المقياس قادراً على توضيح ما هي المخاطر، وآثارها المحتملة وأين قد تنشأ، مع تسليط الضوء بتفصيل كاف على العمليات المنظمية والموارد المهددة. وهذا يمكن الإدارة في تقدير قيمة التحسينات التي أدخلتها لمواجهة المشاكل المخففة قبل ظهورها. وينبغي على المديرين عدم طرح السؤال الآتي: "ما الذي تنوي القيام به حيال هذا"؟ وينبغي على ممارس الأمن توقع مثل هذا السؤال في تقريره. وفي عالم مثالي،

يجب على المديرين بدلا من ذلك طرح السؤال "هل هناك أي شيء يمكنني القيام به؟"

المقاييس المفيدة تتميز بالخصائص التالية:

- تركز على الأعمال: الخيار من المقاييس ينبغي أن يكون بحيث أنها تركز على دعم الأعمال التجارية وذات مغزى لمديري الأعمال. على وجه التحديد، ينبغي أن تكون مقاييس الحوادث الأمنية هي الأهداف الصريحة للمنظمة، عن طريق قياس تجنب التكاليف أو الحد من المخاطر من برنامج الأمن الشامل.
- قابلة للقياس الكمي: تزيد الأرقام موضوعية وصحة البيانات، وتمكن من إجراء المزيد من التحليل والمقارنات.
- يمكن الحصول عليها: يجب أن لا تتطلب بيانات القياسات أدوات معقدة أو إجراءات معقدة للحصول عليها. وينبغي أن تجمع بسهولة من خلال المقابلات أو من البيانات التي تم جمعها من خلال إنجاز الأعمال وعمليات تكنولوجيا المعلومات.
- قابلة للتكرار: يجب أن تكون القياسات قادرة على أن تتكرر بطريقة معيارية في فترات زمنية محددة لتحديد الاتجاهات أو تحديد التغييرات.
- متجهة: القياسات المتكررة تسلط الضوء على التغيير ويسمح لصناع القرار بتقييم فاعلية استراتيجية أمن المعلومات وكيف يتم تطبيقها.

3- نماذج من مؤشرات الأمن ذات الصلة:

Examples of relevant security indicators

المعلومات التاريخية، ولا سيما تقارير المراجعة، يمكن أن تكون مفيدة. وينبغي أن تؤخذ التقارير الأخيرة التي تتضمن توصيات بشأن أمن المعلومات على محمل الجد لأنه:

- (من المفترض أن يكون) أنها تستند إلى وقائع يمكن التحقق منها، وليست مجرد آراء.
- لأنها تعكس احتياجات الأعمال بدلا من الجانب التقني. ومن الناحية المثالية، ترتبط التوصيات بتحليل تأثير أعمال المنظمة وسجل المخاطر.
- تم التوصل إليها من خلال أطر رسمية أنشئت مثل أهداف الرقابة على تكنولوجيا المعلومات (COBIT)، والمبادئ التوجيهية العامة لتدقيق التكنولوجيا (GTAG) من معهد المدققين الداخليين و / أو غيرها من المبادئ التوجيهية.

المعلومات التاريخية الأخرى ذات القيمة يتم إعداد تقارير بها عن التحقيقات التي أجريت بعد وقوع حوادث أمنية خطيرة. وينبغي لهذه المعلومات بيان كيفية وقوع الحادث وأي من نقاط الضعف الذي تم استغلاله. كل المؤشرات التي تدعم المقارنة وتحليل الاتجاهات تعد ذات قيمة من حيث التعريف. ومثال على المقياس المفيد: الوعي الأمني (30٪) من الموظفين الراضين أكملوا البرنامج. وينبغي استكمال تعريف هذا المقياس مع

التفاصيل عن ما هـي الأدلـة الـتي تم جمعهـا ومـا هـو مـصدر البيانـات، تـواتر(تكرار) القياس.

محفظة المقاييس ينبغي أن تكون كبيرة بما يكفي لتكون ذات قيمة ولكـن ليست كـبيرة بحيث يـصبح مـشروعا ضـخما في حـد ذاتـه وتكـون مخرجاته كبيرة جداً يتعذر التحكم بها. يجب أن تشمل الموضوعات الـتي تستحق دعمها مـن قبـل المقـاييس المفيـدة تلـك الـتي تـسهل إعـداد التقريـر بالتغييرات والاتجاهات في مجالات:

- مراجعة إدارة السياسة.
- حالة التنفيذ لتوصيات المراجعة.
- المـوارد البـشرية المسؤولة عـن أنـشطة أمـن المعلومـات ـ علـى سـبيل المثال:
  - حالة تطبيق تدابير الحد من المخاطر الأكبر تاثيراً .
  - مستويات نضج العملية للمهام المتعلقة بأمن المعلومات.
  - الموارد المالية المخصصة لأنشطة أمن المعلومات.
  - إدارة التغيير.
  - اختبارات إدارة الحوادث وخطط إدارة الأزمات.
  - مـدى تطبيـق عناصـر الـتحكم في الوصـول اسـتنادا إلى الـدور (RBAC).

ثانياً : إعداد التقرير عن مقاييس أمن المعلومات

Reporting information security metrics

بالنظر إلى أن هناك كتب مخصصة لمقـاييس الأمـن، فـإن مـا سـنطرحه هنا لا تذهب أبعد من ذلك. الواقع هو أنه من الممكن جمع كميات هائلة مـن

البيانات عن أمن المعلومات، ومعظمها لا تلبي الخصائص المذكورة في أعلاه. الناس المنشغلون في مهام وظيفية يفضلون عادة التقارير المحددة (ad-hoc reports) الصادرة على اساس ما يعرف" الحاجة إلى المعرفة Need To Know ". هذا يعني تحويل مسؤولية تحديد الجهة التي يجب أن تعرف "ماذا ومتى what and when " إلى أؤلئك الذين يقومون بجمع وتحليل البيانات. الكلام أسهل من الفعل. لوحات الخدمة الذاتية الموجودة في الإنترانت تبدو مثل فكرة جيدة ولكن، من الناحية العملية، ليس الكثير لديهم الوقت أو الميل للبحث عن مزيد من المعلومات كما أنها قد تتعرض للإغراق في المعلومات (Information Over-Load) نظراً لكثرة مثل هذه اللوحات. وإتباع نهج معقول يتطلب وجود المسؤولين عن مختلف جوانب أمن المعلومات لتكون الاتصالات بينهم جيدة وتقرير ما يمكن تغطيته عن طريق محادثات غير رسمية في المصعد أو الكافتيريا وما يحتاج إلى تقرير رسمي موجه إلى الأفراد مع السلطة لتأذن باتخاذ الإجراءات المناسبة. و ينبغي أن تكون الإدارة العليا على إطلاع أولاً بأول وبانتظام على ثلاثة مواضيع جوهرية هي:

- الاستخبارات حول التهديدات لأمن المعلومات، و الانجازات الحالية.
- الموارد، ولا سيما في شكل مؤشرات المخاطر الرئيسية (على سبيل المثال " الشخص الرئيسي المسؤول عن أمن المعلومات تقدم بطلب استقالة وليس هناك مرشح واضح لتولي مركزه الوظيفي").
- عدم الامتثال للسياسات والإجراءات.

أسئلة الفصل

س (1): إعكس المقولة التالية على واقع أمن المعلومات: ليس كل ما يهم يمكن عده. ليس كل ما يمكن عده يكون مهماً

س (2): وضح من خلال الشكل مجالات تجسيد أهمية قياس أمن المعلومات. مع فكرة موجزة عن كل منها.

س (3): من وجهة نظرك متى يكون قياس أمن المعلومات مفيداً؟

س (4): يرى الكتاب أنه لكي يكون القياس مفيداً لابد من توفربعض الخصائص، علق على العبارة.

س (5): إذكر نماذج من المؤشرات ذات الصلة بقياس أمن المعلومات.

س (6): محفظة المقاييس يجب أن تشمل الموضوعات التي تستحق دعمها من قبل المقاييس المفيدة، ما هي مجالات هذه الموضوعات؟

س (7): ما هي المواضيع الرئيسة التي ينبغي أن تكون الإدارة العليا على إطلاع عليها أولاً بأول وبانتظام؟

الفصل السابع

موضوعات أمن المعلومات الأخرى

7

- تمهيد
- أولاً: تحليل أثر الأعمال
- ثانياً: إدارة مخاطر المعلومات
- ثالثاً: التخطيط من أجل البقاء
- رابعاً: المشهد التشريعي

الفصل السابع

موضوعات أمن المعلومات الأخرى

Other information security topics

تمهيد:

في هذا الفصل نقدم في شكل ملخص مواضيع أخرى ذات الصلة بأمن المعلومات التي تستحق كتاباً في حد ذاتها، وهذه الموضوعات هي:

- تحليلات أثر الأعمال (BIA).
- إدارة مخاطر المعلومات.
- استمرارية الأعمال وإدارة الأزمات.
- المشهد التشريعي.

أولاً: تحليل أثر الأعمال Business Impact Analysis (BIA)

تحليل أثر الأعمال في أبسط أشكاله، يحدد ما هي أنظمة وخدمات المعلومات ذات الأهمية الحيوية لبقاء المنظمة عندما يحصل حدث تخريبي. ينبغي أيضا أن يحدد كم من الوقت ستستغرق حالة عدم القدرة على أداء العمليات المنظمية لايذاء الأعمال. وبالإضافة إلى ذلك، يجب أيضا أن يحدد أي من الأفراد من داخل المنظمة ومن خارجها والذين تعد المعرفة والخبرة التي يمتلكونها هي الحاسمة عندما تسوء الأمور. ويظهر الشكل (6) مخرجات تحليل أثر الأعمال. حيث تتطلب مثل هذه التحليلات الالتزام والمشاركة النشطة من جانب المديرين الذين لديهم إلمام كافي بالمنظمة وعملياتها. عليه

فإن إجراء هذا التحليل هي مهمة إدارية تتطلب النظر في أبعاد عدة للأثر أهمها:

- التشغيلية: العوامل مثل التأثير على الزبائن، والتميز على المنافسين، التأثير على المنتجين وعلى سلسلة التوريد، والعواقب على القوى العاملة؛
- المالية: التي تتراوح من زيادة الإنفاق لمعالجة اختلال في الخسارة في الإيرادات الناتجة عن عدم القدرة على تقديم الخدمات الى خسارة قيمة السهم.
- التعاقدية والقانونية: عدم القدرة على الوفاء بالتزاماتها التعاقدية مثل تسليم المنتجات؛
- السمعة: وربما من الصعب تقييمها ولكنها مع ذلك مهمة في المدى الطويل.
- المجتمعية: وخاصة في حالة البنى التحتية الحرجة وخدمات الطوارئ حيث يترتب على العطل عواقب كبيرة على السكان عموما.
- وغيرها من التدابير المناسبة لعملك.

ثانياً: إدارة مخاطر المعلومات Information Risk Management

يرى بعض الممارسين أن إدارة المخاطر يجب أن تأتي أولا. ومع ذلك، ومن وجهة نظرنا نرى أنه لا يمكنك الذهاب إلى أي مكان دون أن تعرف أولا من أين تبدأ. ويعد "تحليل أثر الأعمال" الآلية التي توفر هذه المعرفة. هناك العديد من الكتب حول إدارة المخاطر ومخاطرالمعلومات. ومن خلال هذا الشرح

الموجز نسلط الضوء على المفاهيم والعوامل الأكثر أهمية التي تؤخذ في الاعتبار عند تقييم مخاطر المعلومات كجزء من إدارة أمن المعلومات.

وتحتاج عملية "تحليل أثر الأعمال" إلى إعادة النظر بشكل منتظم لتعكس التغيرات في العمليات المنظمية، وأنظمة الحاسبات والخدمات والهياكل التنظيمية. وبمجرد التعرف على الحادث (وليس دائما على الفور) وإعلام مزود الخدمة لتكنولوجيا المعلومات بذلك، وتنطوي الاستجابة لحادث معين على عدة خطوات، وهي:

الخطوة (1): الاحتواء. أي الحد من التأثير من خلال، على سبيل المثال، العزل الالزامي للمرافق المتضررة. وهذا يتطلب من المسؤولين عن الاحتواء الفهم الجيد للمخاطر التي ينطوي عليها القيام (أو عدم القيام) بالعمل.

الخطوة (2): جمع الأدلة والحفاظ عليها. عند التعامل مع الخطوة 1، فإن أي من الادلة التي تم العثور عليها لا ينبغي إتلافها أو التخلص منها. إذ يمكن استخدامها في وقت لاحق لتحديد السبب، وربما تكون هناك حاجة في حالة إتخاذ بعض الإجراءات القانونية. حفظ الأدلة يجب أن يتفق مع المعايير القانونية الوطنية.

الخطوة (3): إعلام أولئك الذين يحتاجون إلى معرفة الحادث. الفشل في القيام بذلك قد يؤخر البت في الحادث، ويعرقل أي تحقيق لاحق. الحوادث الأمنية الخطيرة ترفع كقضايا سرية والتي قد تكون ذات طابع تجاري وقانوني. هذا قد لا يكون كافيا، وأنه قد يكون من الضروري استخدام تدابير أخرى، مثل التعافي من الكوارث، واستمرارية الأعمال وإدارة الأزمات.

مما سبق هناك مجموعة من المخاطر المرتبطة بأنظمة المعلومات وبيئة العمل الخاصة بها، يجب على المؤسسة تحديدها وتقييمها وتطبيق الضوابط المناسبة لتجنبها أو التخفيف من آثارها بالتركيز على مناطق المخاطر الأعلى وكذلك توعية الموظفين بخصوصها وكيفية التعامل معها، وفيما يأتي نستعرض أهم الجوانب ذات العلاقة بخطر المعلومات:

1- المخاطر وعدم التأكد Risk and Uncertainty:

الغموض اللغوي الذي نوقش في وقت سابق، يدفع الكثير من الناس إلى استخدام عبارة "خطر" و "عدم التأكد" بالتبادل، لكنها تعني أشياء مختلفة:

الخطر. هناك العديد من التعاريف التي تعتمد على السياق (في مجال التمويل، والتأمين، والطب، ونظم المعلومات، الخ). تعريف عام واحد هو أنه: "احتمال أو تهديد يلحق الضرر أو الأذى، عائق، فقدان، أو أي واقعة سلبية أخرى والتي تسببها نقاط الضعف الخارجية أو الداخلية، والتي يمكن تجنبها من خلال إجراءات وقائية."

وتعترف معايير أمن المعلومات أن مخاطر أمن المعلومات من الصعب (إن لم يكن من المستحيل) تحديدها كمياً. وذلك لأن تعاريفها لا تشير إلى "الاحتمالية probability". المعيار الدولي (27005:2008 ISO) يعرف الخطر على أنه: "االإحتمالية التي سوف يستغل فيها التهديد لنقاط الضعف في أحد الأصول/ الموجودات، وبالتالي تسبب ضررا للمنظمة." المصطلحات مثل "المحتمل" و "احتمال" تنطوي على إطلاق الأحكام الذاتية تجاه شيء ما، وبناءاً عليه فإن أي تقييمات لمخاطر أمن المعلومات لا تعامل بأنها "حقيقة" ولكن باعتبارها تخمين شخصي. أنه من الجيد أن نتذكر أن عمليات تقييم المخاطر في المجالات الأخرى ـ التعرض لمخاطر العملات الأجنبية، والتغيرات

في سعر السهم والمجالات الاقتصادية الأخرى هي أيضا ليست قوية وتعتمد على نفس الكلمات، "المحتمل" أو "احتمال". وحالة عدم التأكد المقنع هذه تمثل محاولة لمعالجة الأمور التي لا نفهما تماماً.

هذا ليس بالشيئ الجديد، كما نسب الى أرسطو (384 ـ 322 قبل الميلاد) أنه قال: "فمن المرجح أن هناك شيئا ما، من غير المرجح أنه سيحدث". لا يزال هذا القول صحيحا حتى يومنا هذا ويشار اليه على انه" المعروف غير المعروف known unknowns و "غير المعروف غير المعروف unknown unknowns ". وتتطلب الإجراءات الوقائية القدرة على التنبؤ بالمستقبل مع وجود درجة من الدقة، نظرا إلى أن التهديدات يمكن أن تنشأ من القوى الطبيعية (مثل الزلزال وتسونامي فوكوشيما)، الأعمال البشرية العرضية مثل حوادث المرور والحرائق المنزلية، والكشف عن المعلومات السرية في وسائل الاعلام الاجتماعية، والعمل البشري المتعمد (الاحتيال والتخريب والإرهاب وغيرها).

الإجراءات المتعمدة ليست من الأحداث العشوائية، وهذا ما يجعلها لا يمكن التنبؤ بها. ويمكن تخفيض عدم التأكد، عن طريق الاستخبارات (بالمعنى العسكري)، التي يتم الحصول عليها من مصادر جديرة بالثقة الكافية. ومع ذلك، كانت هناك أمثلة عن الاستخبارات التي كان يعتقد أنها جيدة في وقتها، ولكنها في نهاية المطاف تحولت، إلى أن تكون سيئة.

2- إدارة الخطر (الغرض والأنشطة الرئيسة):

Risk Management (purpose and main activities)

يعني الخطر "إمكانية وقوع ضرر أو خسارة **(Conklin et al. 2004)**"، و" الخطر هو حالة عدم اليقين الكامنة في ممارسة الأعمال التجارية، ومن الناحية الفنية، فإن الاحتمال مرتبط بالخسائر أو فشل النظام"، ويقصد

بالخطر " إحتمال وجود حالة غير مرغوب فيها أو حدث غير مرغوب فيه، وتعبر عادة عن الخسارة المحتملة"، و " تحديد المخاطر يتم من خلال فحص وتوثيق الوضع الأمني لتكنولوجيا المعلومات في المؤسسة والمخاطر التي تواجهها. أما التحكم بالمخاطر هو تطبيق ضوابط للحد من المخاطر على بيانات المنظمة ونظام المعلومات". عليه يجب أن تكون هنالك إدارة مختصة بالمخاطر تسمى " إدارة المخاطر" تقوم بعملية تحديد المخاطر، وتقييم المخاطر، وإتخاذ خطوات للحد من المخاطر على مستوى مقبول".

إذن الغرض من إدارة الخطر هو حماية المنظمة من التهديدات التي يمكن أن تعطل أنشطتها. ويعرض الشكل (7 ـ 1) العناصر الرئيسية لإدارة الخطر ومجالات المعلومات اللازمة لإجرائها. وهناك عدة أطر لتقييم إدارة مخاطر المعلومات. ولعل من أهمها هو تخطيط السيناريو (أو ألعاب الحرب war games) والذي يقوم فيها مجموعة من المشاركين الذي يتصفون بالدراية والخبرة باستكشاف حالات "ماذا لو what if " مستخدمين الإبداع (والبعض يقول جنون العظمة paranoia) لوصف كيف يمكن أن تتطور الأفعال المتعمدة ومحاولة توفير مجموعة من الأجوبة على الأسئلة الخمسة (W1H 5). ويمكن لهذا النهج أن يعمل بشكل جيد جدا ويتم تطبيقه على نطاق واسع. ومع ذلك، فهو نهج ليس مثالي. لان هناك عدة عوامل للتقييم مع معلومات غير كاملة، مثل نية التهديد (الطبيعة، عرضية أو متعمدة)، والقدرة، وخاصة إذا كان الإنسان وكان متعمداً، القراصنة الهواة مقابل جيش الكتروني محترف وغير ذلك، فضلاً عن الفرصة، مثل الوصول عن بعد مقابل الأفراد المخولين من الداخل.

ويرى (Mojtahedi et al., 2010) أن تقييم المخاطر ينطوي على تحقيق عدة أهداف هي:

- انه يعطي لمحة عامة عن المستوى العام ونمط المخاطر التي تواجه المشروع.
- تركيز اهتمام الإدارة بشأن البنود ذات المخاطر العالية في القائمة.
- يساعد على تحديد مكان العمل بشكل فوري، وحيث ينبغي وضع خطط عمل للأنشطة المقبلة.
- مرافق تكنولوجيا المعلومات وتخصيص الموارد اللازمة لدعم وإدارة العمل المقرر.

القدرة

الفرصة

النية/ القصد

نوع التهديد
- التهديدات الطبيعية.
- التهديدات البشرية المتعمدة.
- التهديدات البشرية غير المتعمدة.

إدارة الخطر
- تجاهل.
- تجنب.
- قبول.
- تخفيف.
- تحويل.

احتمالية حصول التهديدات

نقاط الضعف في الحاكمية، الأفراد، العمليات،

تحليل أثر الأعمال

الشكل (7 ـ 1)

مكونات الخطر لأمن المعلومات

3- مخرجات إدارة الخطر Risk management outcomes:

مبادرة إدارة مخاطر المعلومات يجب أن تضيف قيمة للمنظمة. للقيام بذلك، يجب ان تتضمن مخرجات مثل هذه المبادرات ما يلي:

- برنامج تفصيلي لإدارة وتخفيف مخاطر المعلومات.
- إدماج المخاطر في برنامج إدارة المخاطر المؤسسية باستخدام التعاريف المشتركة؛
- سجل المخاطر يتضمن وصفا للاستراتيجية التي ستطبق على كل من: تجاهل، وتجنب، قبول أو تخفيف أو نقل؛
- تحديد وتنفيذ تدابير مضادة فعالة لتلك المخاطر.
- تقييم العائد على الاستثمار من التدابير المضادة أينما كان مطلوباً.

ثالثاً: التخطيط من أجل البقاء Planning for survival

حتى المتفائلين من ذوي الخبرة في أمن المعلومات يعترفون بأن حادث أمن المعلومات أمر لا مفر منه وأن ضمان عدم وقوعه (100٪) لا يمكن تحقيقه، والتأهب هو البديل الوحيد عند حدوث الحادث. وهناك عدة مستويات من التأهب بداية مع نظم المعلومات ومقدمي الخدمات. ومجالات المساءلة لهم عادة ما تكون ما يلي:

- آليات لدعم الإبلاغ عن الحوادث، والتحليل والاحتواء والحل.
- أين يكون تقييم أثر الحادث عالياً، وهذا قد يتطلب إنشاء فريق الاستجابة للطوارئ قادر على توفير غطاء (24 ❖ 7).
- تقديم الدعم لفريق التحقيقات ومعرفة كيفية جمع وحفظ الأدلة.
- خطط الطوارئ للسماح للأنظمة والخدمات بالاستمرار في العمل.

- خطط التعافي من الكوارث. وتهدف هذه لتوفير قدرات البنية التحتية والعمليات في موقع آخر. تفترض هذه الخطط أن هذه العمليات لا يمكن أن تستمر في موقعها الأصلي بسبب قوى الطبيعة (مثل الزلازل، وظروف الطقس) أو الإجراءات المتعمدة مثل التخريب، والهجمات الإرهابية، ...إلخ.

وتجدر الإشارة إلى أن خطط التعافي من الكوارث تركز على البنية التحتية المادية، وسوف تكون ذات فائدة محدودة إذا كانت البرمجية أو البيانات تالفة من خلال شكل من أشكال الهجوم الإلكتروني. المستوى التالي من التخطيط لعمليات الاستمرار هو التخطيط لاستمرارية الأعمال ومعالجة حالة عدم توفرالمكاتب المطلوبة، الوصول إلى المباني أو توقفات كبيرة للتسهيلات والمرافق، علماً أن تخطيط استمرارية الأعمال ليست من مسؤولية نظم المعلومات ومقدمي خدمات تكنولوجيا المعلومات.

أما إدارة الأزمات فإنها تعد المكون الرئيسي الثالث من الاستجابة لأحداث أمن المعلومات. وهي تختلف عن السابقتين في أنها ترتبط بالأطراف خارج المنظمة، أي أصحاب المصلحة، وسائل الإعلام وغيرها اعتمادا على طبيعة المنظمة.

رابعاً: المشهد التشريعي The legislative landscape

كما ذكرنا في وقت سابق، تعد إتفاقية مجلس أوروبا بشأن الجريمة الاكترونية أداة راسخة تعالج الطبيعة العابرة للحدود لجريمة الإنترنت. هناك أيضا توجيهات الاتحاد الأوروبي (EC/46/95) بشأن حماية البيانات، هذه التوجيهات تكمل المخططات الوطنية للتشريع. طالما أن الابتكار التقني هو

أسرع من وضع التشريعات ستبقى هناك العديد من المناطق الرمادية. وهذه تختلف من بلد إلى بلد. ومع ذلك يبقى المستشار القانوني للشركات هو المؤهل الأفضل لتحديد التشريعات المعمول بها وإحاطة المسؤولين عن تنفيذ وتشغيل نظم وخدمات االحاسوب بذلك.

أسئلة الفصل

س (1): ما المقصود ب" تحليل أثر الأعمال"، وما هي الأبعاد التي تتطلب النظر فيها؟

س (2): يشير الكتاب الى أن الاستجابة لحادث معين تنطوي على عدة خطوات، وضحها باختصار.

س (3): يختلف مفهوم الخطر عن مفهوم عدم التأكد في أمن المعلومات، هل أنت مع هذا التوجه أم لا ولماذا؟

س (4): تعترف معايير أمن المعلومات أن مخاطر أمن المعلومات من الصعب (إن لم يكن من المستحيل) تحديدها كمياً. لماذا؟

س (5): من أهم الأطر المعتمدة لتقييم إدارة مخاطر المعلومات، تخطيط السيناريو (أو ألعاب الحرب war games)، كيف؟

س (6): عدد أهم الأهداف التي ينطوي عليها تقييم المخاطر لأمن المعلومات.

س (7): وضح من خلال الشكل مكونات الخطرلأمن المعلومات.

س (8): يشير المتخصصون الى أن مبادرة إدارة مخاطر المعلومات يجب أن تضيف قيمة للمنظمة، كيف؟

س (9): حتى المتفائلين من ذوي الخبرة في أمن المعلومات يعترفون بأن حادث أمن المعلومات أمر لا مفر منه وأن ضمان عدم وقوعه (100٪) لا يمكن تحقيقه، ما هو الحل من وجهة نظرك؟

س (**10**): ما هو الهدف من خطط التعافي من الكوارث، وكيف يتحقق؟

س (**11**): تعد إتفاقية مجلس أوروبا بشأن الجريمة الالكترونية أداة راسخة تعالج الطبيعة العابرة لحدود جريمة الإنترنت، كيف؟

الفصل الثامن

آلية تعزيز أمن المعلومات



8

- تمهيد
- الاتجاه الأول: صياغة الاستراتيجية الأمنية
- الاتجاه الثاني: التشريع والقانون
- الاتجاه الثالث: الأفراد العاملون في المنظمة
- الاتجاه الرابع: الإجراءات الصحيحة في التعامل مع الملفات الورقية ومع أجهزة النسخ والفاكس والهاتف النقال والحاسب والمتطفلين
- الاتجاه الخامس: مواجهة الفيروسات
- الاتجاه السادس: تحديد العمليات الرئيسة
- الاتجاه السابع: إنشاء وحدات أمن المعلومات

الفصل الثامن

آلية تعزيز أمن المعلومات

What needs to be done to strengthen security

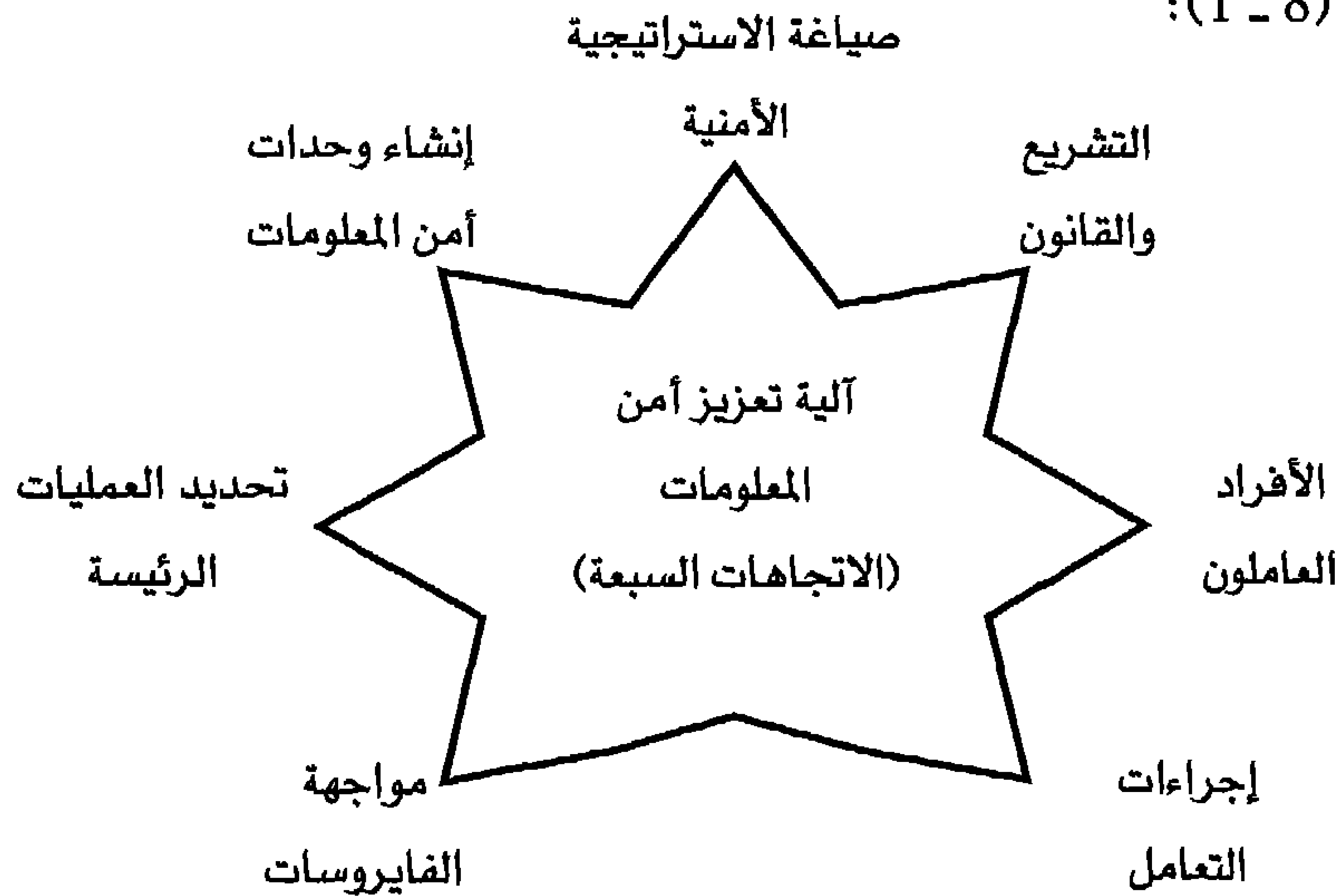
تمهيد:

أكد التقريرالذي نشره مكتب المحاسبة العام الأمريكي (GAO) في ديسمبر (2011) إلى حقيقة جوهرية وهي أن ما يجب القيام به لتعزيز الأمن هو معروف جيدا ولكن ليس جيدا بما فيه الكفاية (What needs to be done to strengthen security is well known but not done well enough)، ذلك لأن إدارة أمن المعلومات تتطلب التركيز على العديد من الأنشطة المتباينة، على وجه الخصوص:

- اختيار واعتماد المعايير والممارسات الجيدة والمبادئ التوجيهية وضمان استيفاءها.
- بناء الوعي لقضايا أمن المعلومات بين الأفراد العاملين ومقدمي الخدمة.
- تحديد أنظمة المعلومات والبيانات الأكثر أهمية، ومواطن الضعف فيها.
- تحديد المدى الذي يتوقع فيه التعرض للمخاطر ومن ثم التخفيف والحد من آثاره.
- تحديد تأثير الأحداث الأمنية على العمليات التجارية والمنظمة ككل.

- تحديد ما تعتبره المنظمة أنه مخاطر مقبولة.
- مراجعة كل ما سبق للتأكد من ملاءمتها.

بناءاً عليه يجب التفكير الجدي بتعزيز أمن المعلومات من خلال اعتماد الآلية الملائمة التي تكفل تحقيق هذا الهدف، وقد اختلف المتخصصون في هذا المجال حول طبيعة هذه الآلية و أبعادها إلى الحد الذي يتعذر معه الحديث عن أساليب معيارية موحدة يمكن اعتمادها من قبل مختلف المنظمات بغض النظر عن طبيعة أنشطتها وحجمها وأهدافها وفلسفة إداراتها وطبيعة تكنولوجيا المعلومات المعتمدة من قبلها (Shapira,1993:37). ومع ذلك فانه يمكن الاسترشاد بهذه الآراء لبلورة بعض المقترحات التي تشكل الإطار لآلية تعزيز أمن المعلومات في المنظمات المختلفة، ولأجل تسهيل مهمة تحديد أبعاد هذه الآلية فقد ارتأينا تصنيفها من خلال الاتجاهات الآتية الموضحة في الشكل (8 ـ 1):

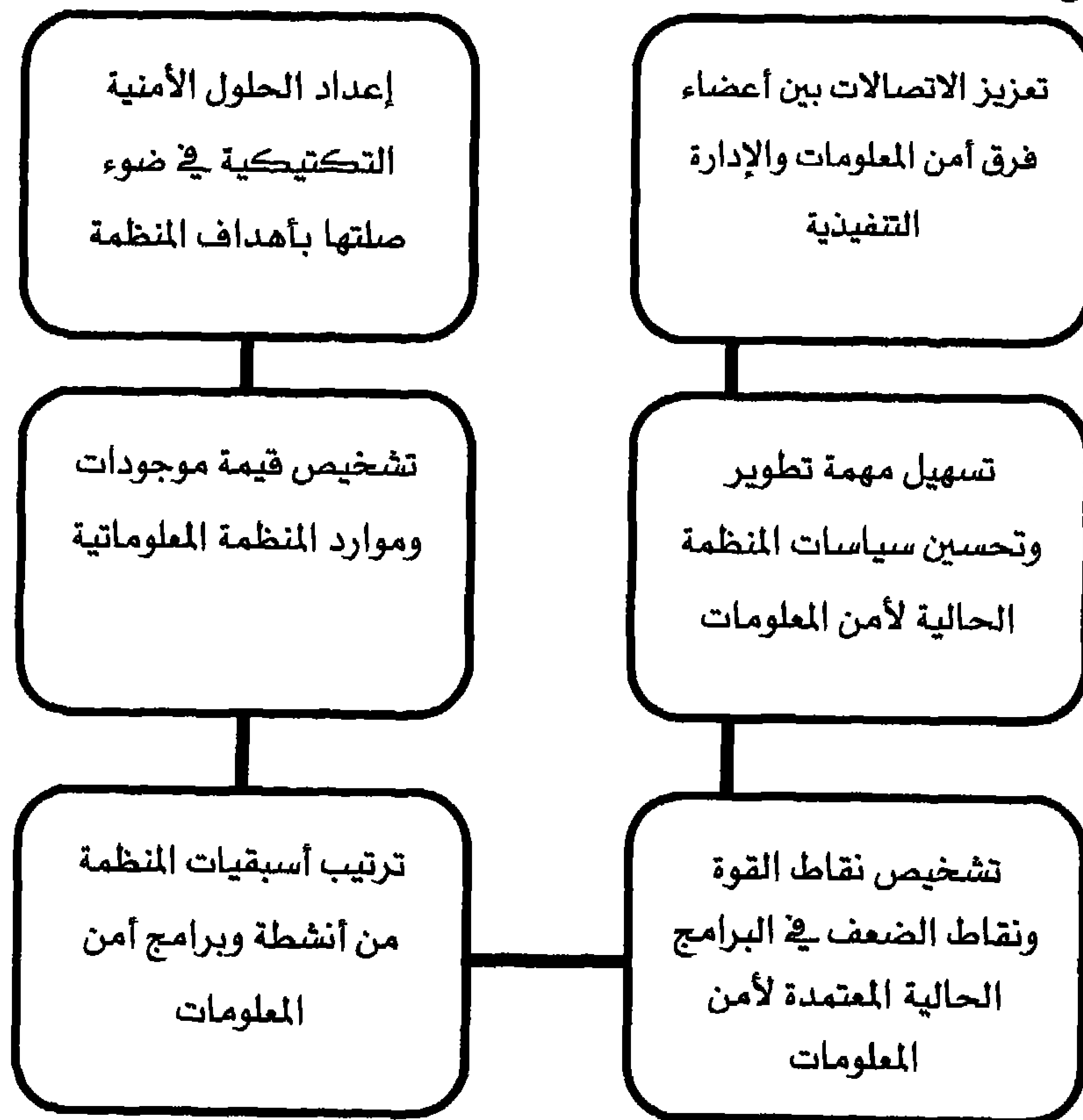


الشكل (8 ـ 1)

الاتجاهات السبعة في إطارآلية تعزيز أمن المعلومات

الاتجاه الأول: صياغة الاستراتيجية الأمنية

تؤمن وجود الاستراتيجية الملائمة لامن المعلومات في توفير المناخ السليم لتحقيق هذا الأمن وتعزيزه وذلك من خلال الجوانب الاتية الوضحة في الشكل (8 ـ 2). (almer, 2001 : 13):



الشكل (8 ـ 2)

دور الاستراتيجية الملائمة في توفير المناخ السليم لأمن المعلومات

ويقترح (الطائي، 2000: 294 ـ 308) إطارا عاما لهذه الاستراتيجية على وفق الأبعاد الآتية:

- صياغة الرؤية الاستراتيجية لنظام الحماية الأمنية والتي تحدد الوضع الحالي لنظام الحماية وما يجب أن يكون عليه هذا النظام مستقبلاً.
- تحديد القواعد الأساسية لنظام الحماية والتي يمكن الاسترشاد بها وهذه القواعد هي قاعدة قبول الحماية وقاعدة النقاط الحرجة وقاعدة المسؤولية القانونية.
- تحديد أساليب الحماية الأمنية الإدارية والتي تشتمل على حماية مركز الحاسب والتحكم بالدخول إلى هذا المركز وحماية الأقراص والأشرطة والبرامج والتجهيزات والحماية من الحريق.
- تحديد أساليب الحماية الأمنية التشغيلية والتي تضم حماية المدخلات وحماية عمليات المعالجة وحماية المخرجات وحماية قاعدة المعلومات.

الاتجاه الثاني: التشريع والقانون

ويقع ضمن اهتمامات وصلاحيات رجال القانون وذلك من خلال إصدار التشريعات والقوانين التي تحد من الخروقات الأمنية على النحو الذي يلحق الضرر بالمنظمات. إذ تعد جريمة سرقة المعلومات جريمة العصر بحق بعد أن انتشرت وتوسعت وتعددت طرقها وفنونها مع التوسع الكبير في استخدام الحاسب وملحقاته في تطبيقات نظم المعلومات على النحو الذي أثار قلق المشرعين القانونين، ويشير هنا أحد الخبراء في مجال القانون إلى أن سرقة المعلومات أصبحت أسرع الجرائم انتشارا في عصرنا الراهن مع تطور المجتمع

وتحوله إلى مجتمع تكنولوجي في أغلب مناحيه ومما يزيد الأمر تعقيداً هو الآتي: (الطائي، 2000)

1- أن القانون يمضي متخلفا عن هذه التطورات التكنولوجية بخطوات كبيرة، فالقانون لا يعامل المعلومات كسلعة ذات قيمة كبيرة.
2- فضلا عن أن القانون في الكثير من الدول لا يعاقب على هذا النوع من الجرائم.
3- كما لا يتيح القانون الفرصة أمام الجهات القضائية بملاحقة هؤلاء المجرمين قانونيا.

لقد كان هذا الموضوع مثار مناقشات حادة اشتركت فيها الوكالات الحكومية القانونية الأمريكية حول التوصل إلى الإجراءات القانونية التي تحد من حالات الخروقات وتسهم في كشف الأدلة التي تساعد السلطات القضائية من إصدار العقوبات الرادعة وتطبيق تلك الإجراءات.

الاتجاه الثالث: الأفراد العاملون في المنظمة

على الرغم من عدم كمال إجراءات أمن الحاسب والمعتمدة حاضراً من قبل اغلب المنظمات إلا أن هذه الإجراءات فاعلة بما فيه الكفاية في حماية المعلومات المخزونة على الحاسب ولكن يبقى الأفراد المستخدمون العامل الأساس في أمن المعلومات وليس الحاسب، إلى الحد الذي يمكن القول معه أنه لا قيمة لأي نظام أمني مهما كانت التكنولوجيات المستخدمة فيه متطورة في حالة فشل مستخدموا هذا النظام في إتباع الإجراءات الملائمة لتنفيذه. بناء عليه فإن الالتزام ببرنامج آمني فاعل للمعلومات يجب ان يبدأ من العاملين في المنظمة وفي مقدمتهم الإدارة العليا نزولا إلى المستويات الأخرى

(Richards-Carpenter,1993). ويعـد الـوعي بأهميـة وخطـورة أمـن المعلومـات الأساس في تحقيق مثل هـذا الالتـزام إلى جانـب إدراك أهميـة دورهـم في حمايـة المعلومات ومن ثـم معرفـة أهميـة تحمـل مسـؤلية ذلـك حتـى في مجـالات الحيـاة اليوميـة الاعتياديـة والتعامـل مـع هـذه المعلومـات بطريقـة مقبولـة، فـالإدراك والمعرفة يمثلان نصف المعركة حيث أنـه بمجـرد أن يـصبح الأفـراد مـدركون لأهمية قيمة المعلومات عندها تصبح مهمـة تطبيـق الإجـراءات الخاصـة بالنظـام الأمـني سـهلة وممكنـة (Wood & Banks ,1993). ويجمـل (الطـائي، 2000) أهـم هذه الإجراءات بالآتي :

- التحري الدقيق عن الأفراد العاملين الـذين سيشغلون مناصـب معينـة في إدارة وتـشغيل وحـدة نظـام المعلومـات قبـل الإقـدام علـى اختيـارهم وتعيينهم وتثبيتهم في وظائفهم.
- فصل المهام عن بعضها البعض وخاصة تلك الـتي تسهل وتـشجع علـى اختراق أمن المعلومات، ومنع العملين من استخدام اكثر مـن طرفيـة واحدة لتغذية الحاسب.
- الاهتمـام بـالأفراد العـاملين ورفـع روحهـم المعنويـة مـن خـلال تـوفير الأجـواء الملائمـة والاهتمـام بمشاكلهم وسمـاع آرائهـم ومقترحـاتهم وتعزيز المكافآت الممنوحة لهم.
- الإجراء القانوني الذي يتمثل في وجود مادة قانونية تنص على معاقبـة الأفراد الذين يسهلون مهمة اختراق أمنالمعلومات في إطار مسئوليتهم القانونية.

الاتجاه الرابع: الإجراءات الصحيحة في التعامل مع الملفات الورقية ومع أجهزة النسخ والفاكس والهاتف النقال والحاسب والمتطفلين

وذلك من خلال تجاوز العيوب والثغرات التي تشكل الفرص السانحة لاختراق أمن المعلومات في هذه المجالات وعلى النحو الآتي:

1- الملفات الورقية:

إن أمن المعلومات في الملفات الورقية يمكن تحقيقها بسهولة فيما إذا أدرك الأفراد المتعاملون معها - وخاصة تلك الملفات المصنفة على أنها سرية - مدى الحاجة لأمن المعلومات. وهناك مجموعة من الإجراءات التي يمكن أن تضمن أمن هذه الملفات وهي (Leyzorek ,1991):

- منع وصول الأفراد غير المرخصين إلى هذه الملفات والسعي إلى تصنيف الملفات إلى ملفات سرية وغير سرية وحفظ السرية منها في مواقع أمينة أو في خزانات مقفلة.
- عدم استنساخ أكثر من النسخ المقررة سواء كانت المعلومات حساسة أم لا مع الحذر الشديد لاسترداد النسخ الأصلية بعد الانتهاء من عملية النسخ.
- عدم رمي النسخ رديئة الطبع والتي تحتوي على معلومات مهمة في سلة المهملات قبل تمزيقها بشكل مناسب من خلال استخدام مكائن خاصة معدة لهذا الغرض.
- الحذر والانتباه عند اختيار من يطلع على بحوث المنظمة الداخلية وأدلتها ونشراتها وأخبارها الداخلية، وإذا لم يكن هناك من بد من نشر المعلومات فإنها يجب أن تنشر في إطار عام وليس تخصصي.

2- الفاكس:

إن أفضل طريقة للتعامل مع أجهزة الفاكس تتمثل في الإجراءين الآتيين:

- الانتباه عند إرسال معلومات سرية إلى أجهزة الفاكس ذات الاستخدام العام وتجنب استخدام الفاكس في المراسلات التي تتصف بالسرية، وإذا كان لابد من ذلك فانه يجب على إدارات المنظمات اتخاذ المزيد من إجراءات الرقابة لمنع الوصول العام إلى أجهزة الفاكس وذلك بتكليف أفراد مهمتهم مراقبة الجهاز بشكل مستمر أو وضع أجهزة الفاكس في غرف مقفلة لا يدخلها إلا الأفراد المخولون.
- السعي إلى استخدام أجهزة خاصة لمنع حدوث المراقبة غير المرخصة لأجهزة الفاكس التابعة للمنظمة.

3- الهاتف النقال:

يرى (Menkus,1990) أن أفضل إجراء يمكن اعتماده لتجاوز الخروقات الأمنية في الهاتف النقال هو تجنب مناقشة الأمور الهامة والامتناع عن التحدث بالمعلومات الحساسة التي قد يؤدي تسريبها أو إساءة استخدامها إلى إلحاق الضرر بالمنظمة.

4- التجسس:

يمكن الحد من حالات التجسس أو التقليل من آثارها السلبية من خلال اعتماد الإجراءات الآتية:

- عدم السماح بإجراء الجولات السياحية للمنظمة إلا في حالات الضرورة القصوى.
- حصر الزائرين الغرباء في منطقة محددة معروفة ومراقبتهم عن كثب طيلة الوقت.
- تجنب إعطاء الكثير من المعلومات عن المنظمة لطالبي الوظائف.
- تجنب التغافل عن كوادر الخدمات الخارجية مثل شركات التنظيف ومكاتب الصيانة وما شابهها.
- تجنب إغفال الأفراد العاملين الساخطين أو الذين أنهيت خدماتهم.

5- الملفات الإلكترونية:

لأجل تحقيق أمن هذه الملفات ينصح اغلب المختصين باعتماد إجراءين على الأقل ويتم تعزيزهما بإجراءات إضافية أخرى وهما:

- استخدام كلمة السر بهدف الوصول إلى النظام ابتداء ومن ثم يتم الاستخدام.فعلى الرغم من أن بعض الإجراءات المستندة على الحاسب تعطي اهتماما خاصا لكلمات السر إلا انه لا يزال العديد من المستخدمين لا يعيرون الاهتمام والجدية الكافية وقد يعدها البعض غير ملائم كإجراء أمني، من هنا ولأجل تفعيل هذا الإجراء يجب على المستخدمين الالتزام ببعض القواعد الخاصة باستخدام كلمة السر ومن أهمها عدم إشراك الآخرين فيها حتى ولو كانوا موضع الثقة، وتجنب وضع كلمات العبور ذات المعنى في الحياة اليومية، والسعي إلى تغيير كلمة السر بشكل منتظم إلى جانب

تجنب الاحتفاظ بنسخ مكتوبة منها على المكاتب بالقرب من الحاسب وأيضا تجنب تقليد كلمة السر على أرقام الهاتف.

- تدقيق ما تمت من عمليات لتسهيل مهمة كادر أمن المعلومات من متابعة أية تغييرات حصلت على المعلومات وتأشيرة أين ومتى تم إحداث هذه التغييرات.

أما الإجراءات الأمنية الأخرى فتتمثل في:

- استخدام الطرفيات التي يمكن إقفال لوحة مفاتيحها أو الاحتفاظ بها في غرف مقفلة لمنع الوصول إليها.
- استخدام الحاسب ذات الأقراص الصلبة ممكنة الاستبدال بحيث يمكن رفع القرص الصلب والاحتفاظ به في مكان مقفل وأمين.
- تقليص كمية المعلومات الحساسة المخزونة على الحاسب إلى أدنى حد ممكن.
- اتخاذ إجراءات التحوط تجاه سرقة الجهاز إما بالاحتفاظ به داخل الأمتعة بشكل يتعذر رؤيته أو حمله بطريقة يتعذر سرقته.
- استخدام برامج السرية (Encryption Programs) وهي الخوارزميات التي تمزج وتجانس محتويات مجاميع المعلومات وتناغم الملفات أو تعالج الملفات والبريد الإلكتروني وتغلق الحاسب أمام محاولات خرق سرية المعلومات، إذ تعمل هذه البرامج باستخدام مفتاح خاص لمجانسة الخصائص في الملف أو الشبكة مما يتيح خليطا من المعلومات غير المفهومة إلا من قبل الأفراد المتلقين المقصودين والمخولين بالإطلاع عليها.

الاتجاه الخامس: مواجهة الفيروسات

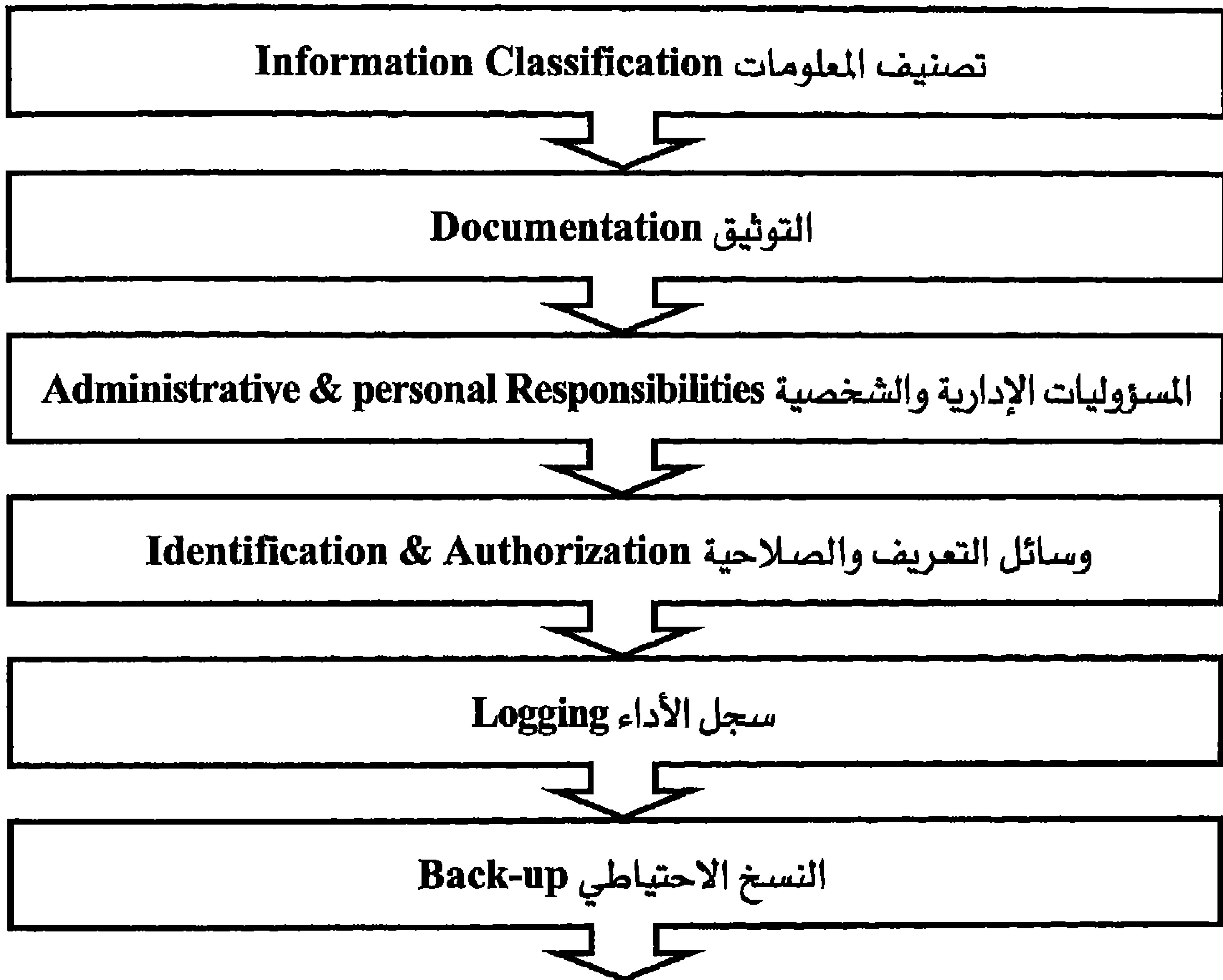
تستخدم المنظمات حالياً العديد من الإجراءات العملية التي تسهم في الكشف عن الفيروسات بسرعة ومعالجتها وتطهير ذاكرة الحاسب والتخلص من الأقراص والأشرطة الملوثة بالفيروس وهذه الإجراءات بحاجة إلى تحسين وتطوير مستمرين بسبب خطورة هذه الفيروسات وبسبب الأهداف التي يسعى إلى تحقيقها المتعاملون معها، من هنا فان الخطوة الأفضل هي الوقاية من الفيروس وممارسة إجراءات الحماية التي تتضمن الآتي (Roy, Jin & Roy ,1991):

- إيجاد نسخ إضافية للبرمجيات والملفات المستخدمة والتي قد تتعرض للإصابة بالفيروس.
- تأمين مواقع بعيدة لتخزين النسخ الاحتياطية عن مواقع الأجهزة الحالية.
- منع استخدام الأقراص والأشرطة من خارج المنظمة وخاصة المجهولة منها إلا بعد التأكد من خلوها من الفيروسات وأيضا التحقق من مصدرها الأصلي.
- اعتماد رموز خاصة بالبرمجيات المستخدمة في النظام على النحو الذي يتعذر فيه الاستفادة منها حتى في حالة نسخها مع التشديد على تجنب استخدام كلمات سر النظم الشائعة، إذ أن لبعض الفيروسات قدرة الوصول إلى النظام من خلال المحاولات مع كلمات السر لحين الوصول إلى الكلمة المطلوبة.
- مراقبة الحاسب باستمرار للتأكد من عدم وجود فيروس مختبئ مع التأكيد على استخدام مضادات الفيروس.

- حصر مسؤولية أمنية أجهزة ومواقع الحاسب وملحقاته بجهة محددة.

الاتجاه السادس: تحديد العمليات الرئيسة

يمكن بوجه عام تحديد العمليات الرئيسية التالية للتعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات، وهذه العمليات يوضحها الشكل (8 ـ 3).

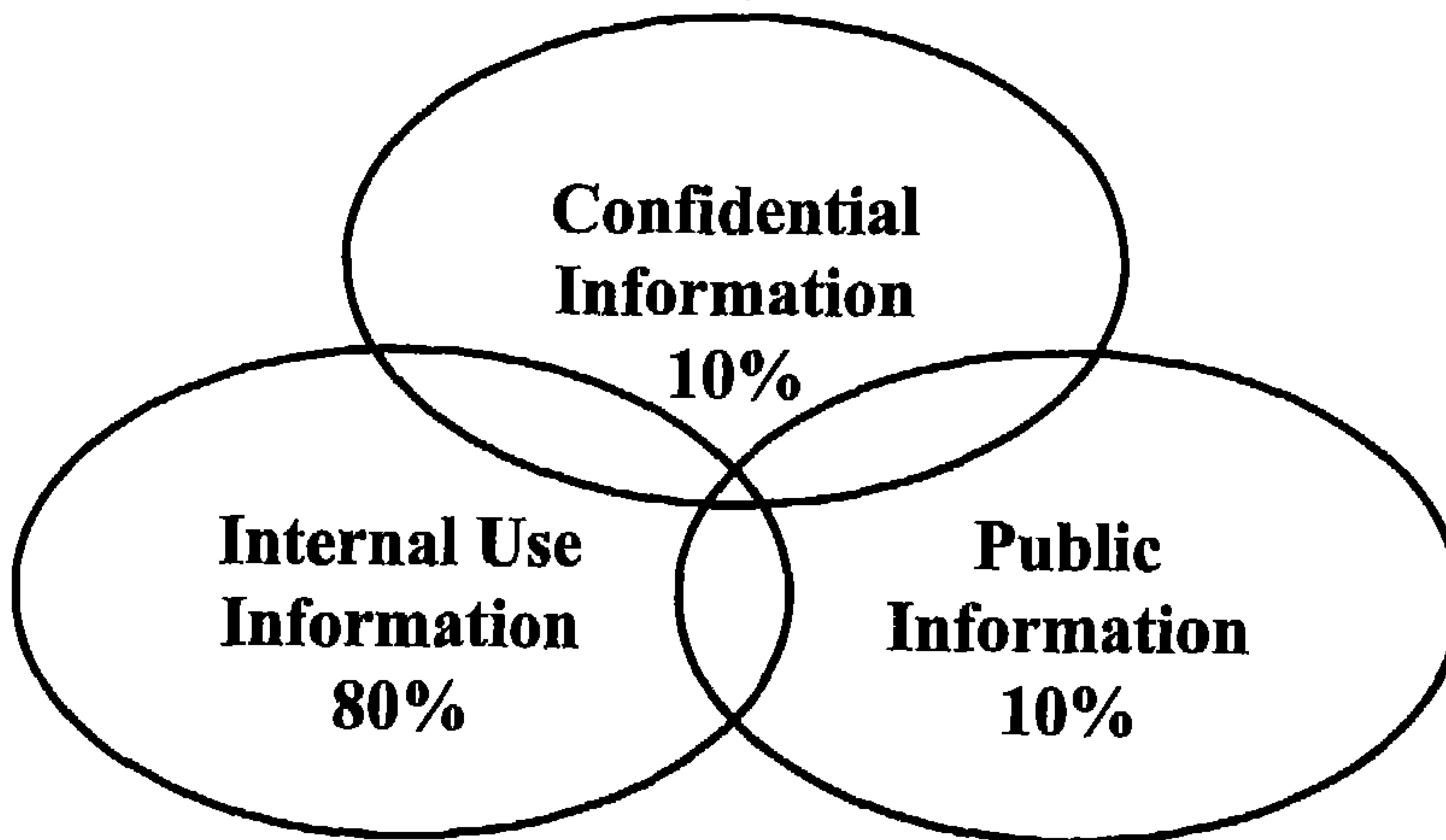


الشكل (8 ـ 3)

العمليات الرئيسة للتعامل مع أمن المعلومات في بيئة النظم

1- تصنيف المعلومات Information Classification:

يشير (E Whiteman & J Mattord,2012) إلى أن "العديد من الشركات تستخدم نظام تصنيف المعلومات للمساعدة في تأمين سرية وسلامة المعلومات، نلاحظ أن " كل المعلومات يتم توليدها ولكن ليس كل المعلومات لها نفس القيمة "All information is created equal, but not all information is of equal value." ، بالتالي لابد أن يكون هنالك تصنيف للمعلومات، " وهي عملية أساسية عند بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأة مدار البحث (المركز الوطني للتوثيق، 2012)، ويشير (Peltier, 2004) في الشكل (8 ــ 4) إلى تصنيفات المعلومات، و" يجب أن تصنف جميع المعلومات في المنشأة إلى واحدة من التصنيفات الثلاثة: السرية، الاستخدام الداخلي، الاستخدام العام، متاحة من حيث الوصول اليها وممكن ان يكون ممنوع الوصول إليها إلا من قبل أشخاص مخولين بذلك.



الشكل (8 ـ 4)

تصنيف المعلومات

2- التوثيق Documentation:

يؤكد المركز الوطني للتوثيق بخصوص أمن المعلومات على أن " عمليات المعلومات تتطلب أساساً اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها ، وبشكل رئيس فإن التوثيق يعد ضروري لنظام التعريف والتخويل، وتصنيف المعلومات، والأنظمة التطبيقية، وفي إطار الأمن، فإن التوثيق يتطلب أن تكون إستراتيجية أو سياسة الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر والحوادث، والجهات المسؤولة ومسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر (المركز الوطني للتوثيق، 2012).

3- المسؤوليات الإدارية والشخصية:

Administration and Personal Responsibilities

يمكن أن نطلق مفهوماً آخراً وهو الفصل في المهام أو الواجبات "وهو مبدأ للعاملين في العديد من المؤسسات لضمان عدم قيام شخص واحد على إجراء جميع الأعمال لوحده، وهذا يعني تقليل مستوى الثقة بشخص واحد ، والتخفيف من أعباء العمل من جهة أخرى، وعدم قدرة الشخص الواحد بالقيام بأي أضرار كارثية للمؤسسة التي يعمل فيها (Conklin, et al. 2004)، "ويتم تقسيم الأنشطة في المؤسسة إلى عدة أشخاص، الأخطاء التي إرتكبها شخص واحد تميل إلى أن تحدد من قبل الشخص التالي في السلسلة، وهذه العملية تزيد من سلامة المعلومات (Peltier,2004)، من جهة أخرى يؤكد المركز الوطني للتوثيق أمن المعلومات على " أن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حُسن إختيار الأفراد المؤهلين وعمق معارفهم

النظرية والعملية، على أن يكون مدركاً أن التأهيل العملي يتطلب تدريباً متواصلاً ولا يقف عند حدود معرفة وخبرة هؤلاء لدى تعيينهم، وبشكل رئيس فإن المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسية : تحليل المخاطر، وضع السياسة أو الإستراتيجية، وضع خطة الأمن، وضع البناء التقني الأمني، توظيف الأجهزة والمعدات والوسائل، وأخيرا تنفيذ الخطط والسياسات (المركز الوطني للتوثيق، **2012**).

ومن المهم إدراك أن نجاح الواجبات الإدارية أو الجماعية للمنشأة يتوقف على إدراك كافة المعنيين في الإدارة (بمهامهم التقنية والإدارية والمالية) إستراتيجية وخطة وواجبات الأمن وإلتزام المؤسسة باعتبار مسائل الأمن واحداً من الموضوعات التي يدركها الجميع ويتمكن الكل من التعامل مع ما يخص واجباتهم من بين عناصر الأمن.

وعلى المستوى الشخصي أو مستوى المستخدمين، فإن على المؤسسة أن تضع التوجيهات الكافية لضمان تحقيق وعي تام ودقيق بمسائل الأمن، بل المطلوب بناء وتكريس ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الإجراءات المتطلبة من قبل الجميع لدى ملاحظة أي خلل، وعلى المؤسسة أن تحدد للمستخدمين ما يتعين عليهم القيام به في معرض استخدامهم للوسائل التقنية المختلفة.

4- وسائل التعريف وصلاحيات الاستخدام:

Identification and Authorization

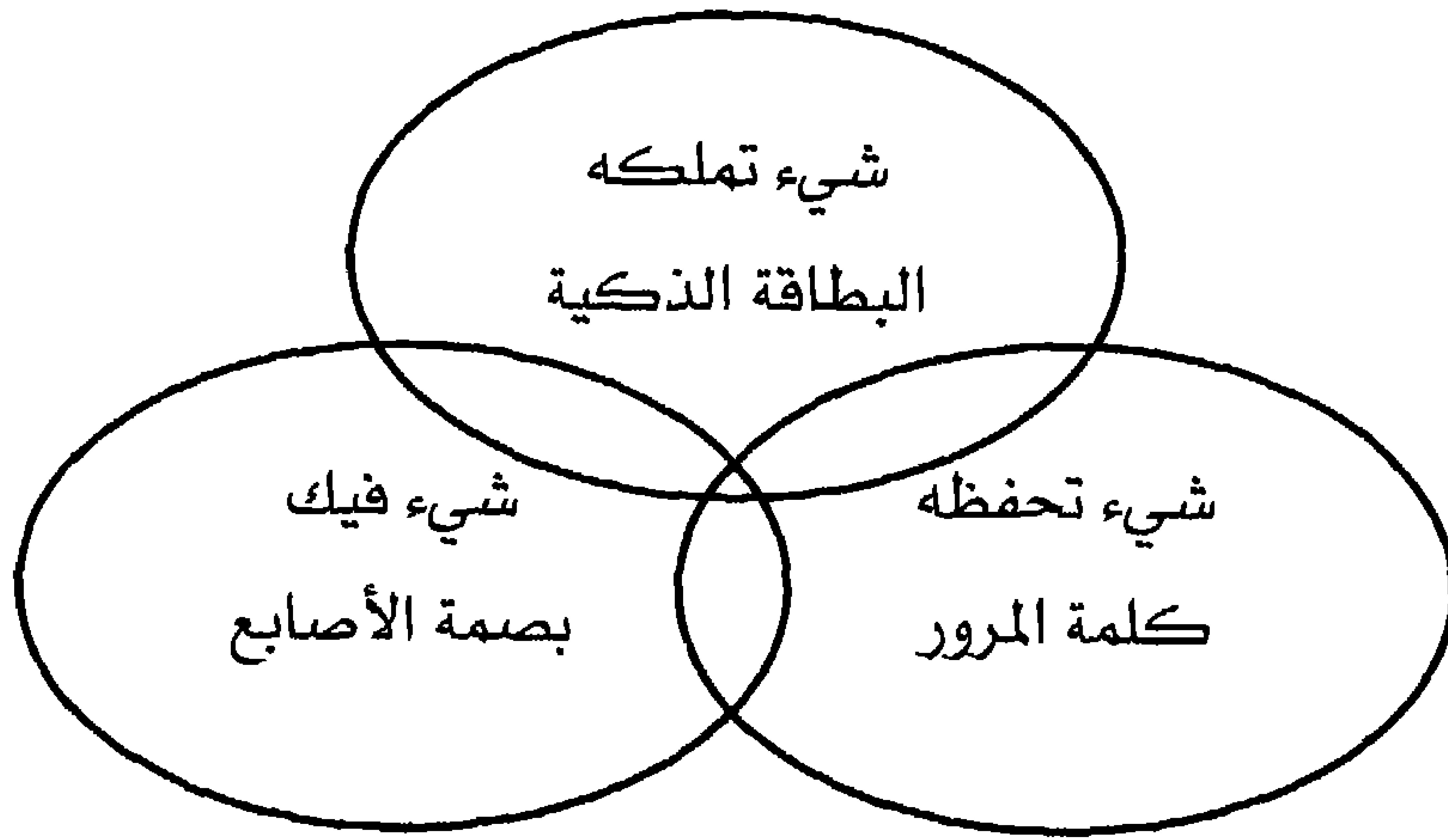
الهدف من وسائل التعريف والتوثيق " التأكد من المستخدمين والأنظمة و طريقة معالجة البيانات قبل تقديم الخدمة أو إعطاء البيانات للعملاء **(Tipton, & Krause, 2005)**، و" التثبت من الهوية وتحديداً عندما يقوم شخص

ما بالتعريف عن نفسه، حيث أن الدخول إلى أنظمة الحاسوب وقواعد البيانات ومواقع المعلوماتية عموماً، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام، وهو ما يعرف بأنظمة التعريف والتخويل Identification and Authorization System.

والتعريف أو الهوية مسألة تتكون من خطوتين، الأولى وسيلة التعريف على شخص المستخدم، والثانية قبول وسيلة التعريف أو ما يسمى التوثق من صحة الهوية المقدمة، وهي " التخويل التي تعني عملية السماح أو منع الوصول إلى المصادر المحددة (Conklin,etal.2004)". ويشير (Lehtinen&Russell,2006) إلى أن " الحفاظ على الأنظمة عادة يتم من خلال توفر ملف يحتوي على الصلاحيات والخصائص الخاصة بالمستخدم، في بعض الأنظمة، يسمى هذا الملف بملف تعريف الأمن، أو بتعريف التخويل، أو قائمة المستخدم (Lehtinen et al, 2006,)".

ووسائل التعريف تختلف تبعاً للتقنية المستخدمة، وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات إستخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية، وهذه الوسائل تقسم إلى ثلاثة أنواع (Conklin, et al. 2004)، كما هي موضحة في الشكل (8 ـ 5) وهي:

- شيء ما يملكه الشخص مثل البطاقة البلاستيكية أو غير ذلك.
- شيء ما يعرفه الشخص مثل كلمات السر أو الرمز أو الرقم الشخصي أو غير ذلك.
- شيء ما يرتبط بذات الشخص أو موجود فيه مثل بصمة الإصبع أو بصمة العين والصوت وغيرها.



الشكل (8 ـ 5)

الوسائل الثلاث الأساسية للتعرف على هوية المستخدم

ممكن أن نلقي الضوء على بنك القاهره عمان، الذي أدخل على نظامه المصرفي تقنية جديدة من خلال الصراف الآلي دون الحاجة إلى وثيقة إثبات الشخصية، " من خلال بصمة العين، تقنية آمنة ودقيقة يستحيل تزويرها كونها أكثر أماناً من البطاقات والأرقام السرية المعرضة للسرقة أو النسخ أو التزوير (موقع بنك القاهره عمان، 2012).

وأفضل استخدام لوسيلة من الوسائل السابقة هو أن تجمع ما بين الوسائل المختلفة لتوثيق أعلى كفاءة، وملاحظة أن كلمات السر هي الأكثر شيوعاً، يجب مراعاة عدد من الشروط عند كتابة كلمة السر للحفاظ عليها ولعدم كشفها من قبل أشخاص غير مخولين بذلك.

5- سجل الأداء (النفاذ) Logging:

تحتوي مختلف أنواع الحاسبات نوعاً ما من السجلات التي تكشف إستخدامات الجهاز وبرمجياته والنفاذ اليه، وهي ما تعرف بسجلات الأداء أو

سجلات النفاذ إلى النظام، وتكتسب سجلات الأداء أهمية إستثنائية في حال تعدد المستخدمين وتحديداً في حالة شبكات الحاسوب التي يستخدم مكوناتها أكثر من شخص، وفي هذه الحالة تحديداً، أي شبكات المستخدمين، فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات، كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها، فهناك سجلات الأداء التاريخية والسجلات المؤقتة، وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة أو ما يعرف بسجلات الأمور التقنية وغيرها" (المركز الوطني للتوثيق، 2012).

وبشكل عام فإن سجلات الأداء منوط بها أن تحدد شخص المستخدم، ومكانه، وطبيعة الاستخدام (محتواه) وأية معلومات إضافية أخرى تبعاً للنشاط ذاته.

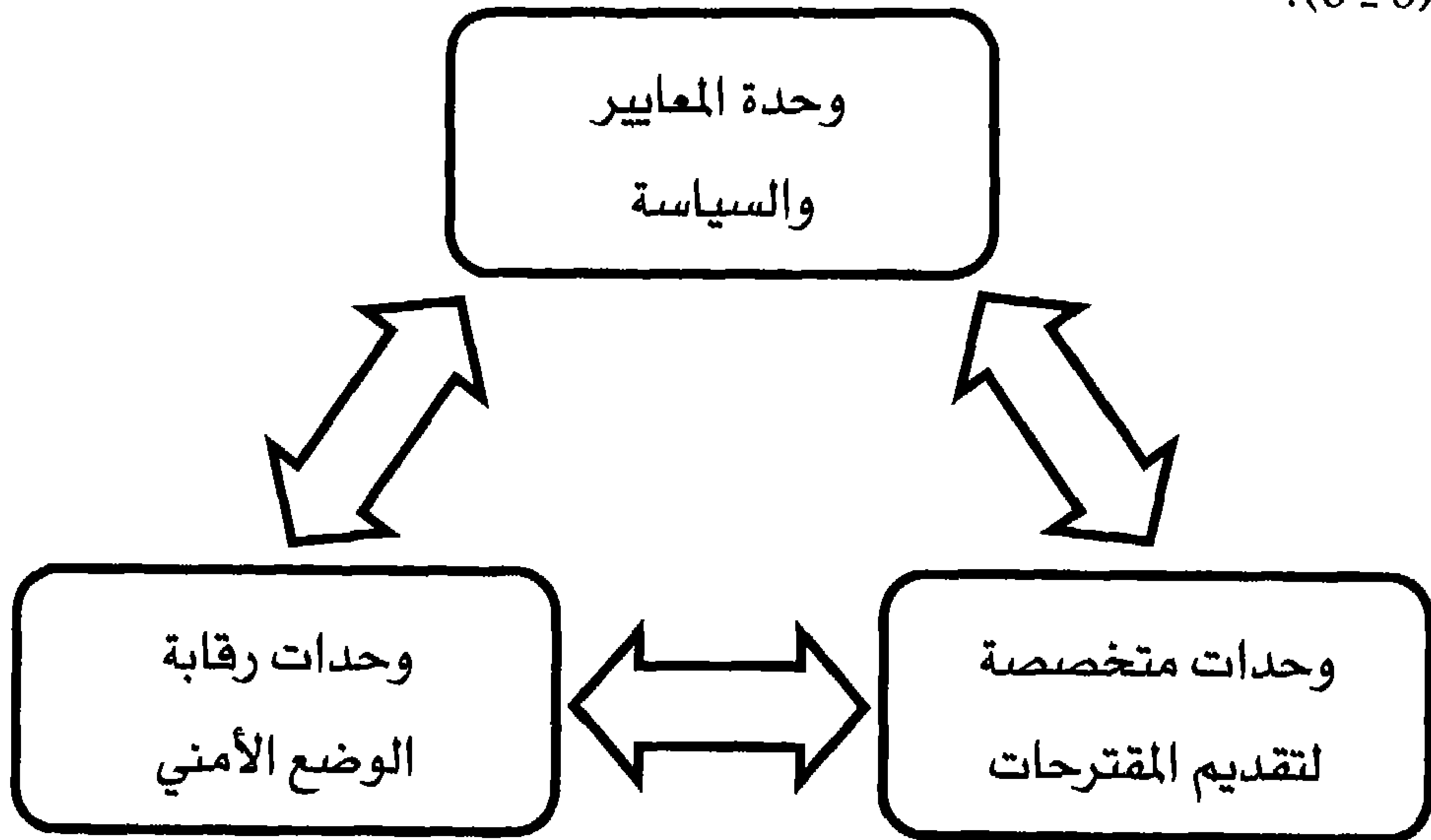
6- النسخ الاحتياطي Back-up:

عمليات الحفظ الإحتياطي للبيانات تتم من خلال نسخ المعلومات الرقمية إلى وسائط تخزين مختلفة ويفضل أن يكون في مكان خارج الموقع بحيث يمكن إستخدامه في حال وقوع كارثة" (CIMPA & REVELS, 2013) و"عمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه، وتخضع عمليات الحفظ لقواعد يتعين أن تكون محدده سلفاً وموثقه ومكتوبه ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية" (المركز الوطني للتوثيق، 2012). " هذا صحيح ليس فقط بسبب إحتمال وقوع كارثة، لكن

بسبب أن بعض الأجهزة أو البرمجيات ممكن أن تتعطل، نتيجة لذلك يتم فقدان أو تلف البيانات المهمة" (Conklin, et al. 2004). ويمثل وقت الحفظ، وحماية النسخة الاحتياط، ونظام الترقيم والتبويب، وآلية الاسترجاع والاستخدام، ومكان الحفظ وأمنه، وتشفير النسخ التي تحتوي معطيات خاصة سرية، مسائل رئيسية يتعين إتخاذ معايير واضحة ومحددة بشأنها.

الاتجاه السابع: إنشاء وحدات أمن المعلومات

يرى (Parker , 1997 :15) ضرورة استحداث ثلاثة وحدات تنظيمية تتولى مسؤولية توفير أمن المعلومات وهذه الوحدات هي كما موضحة في الشكل (8 ـ 6):



الشكل (8 ـ 6)

الوحدات التنظيمية المسؤولة عن أمن المعلومات

- وحدة المعايير والسياسة والتي ترفع تقاريرها إلى الإدارة العليا وقد تنجز هذه الوحدة أيضا عمليات تقويم ومراجعة الوضع الأمني للوحدات المنظمية الفرعية وترفع التقارير بشأن الخروقات الأمنية التي يتم الكشف عنها.
- وحدات متخصصة لتقديم المقترحات. قد تكون واحدة أو اكثر" تقام في التشكيلات المنظمية الفرعية لغرض تقديم المقترحات بشان التطوير المستمر للإجراءات الرقابية المعتمدة وتشغيلها وصيانتها.
- وحدات رقابة الوضع الأمني. وتتألف من شبكة من االأفراد العاملين الذين يعملون بدوام جزئي أو كامل وبصفة منسقين أمنيين في كل تشكيل منظمي فرعي وتختص هذه الشبكة برقابة الوضع الأمني داخل هذه التشكيلات وكذلك إيصال المعلومات الأمنية إلى العاملين في مجال المعلومات في تلك التشكيلات المنظمية.

أسئلة الفصل

س (1): وضح من خلال الشكل الاتجاهات الرئيسة لآلية تعزيز أمن المعلومات.

س (2): وضح من خلال الشكل دور الاستراتيجية الملائمة في توفير المناخ السليم لأمن المعلومات.

س (3): ضع دائرة أمام الاجابة المناسبة

يمكن إعتماد الآلية المناسبة لتعزيز أمن المعلومات في المنظمة من خلال مراعاة:

A- فلسفة المنظمة وأهدافها وأنشطتها	B- حجم المنظمة وتشكيلاتها التنظيمية
C- التكنولوجيا المعتمدة فيها	D- جميع ما ذكر صحيح

س (4): عدد أهم الأبعاد المقترحة لتشكيل الإطار العام لاستراتيجية أمن المعلومات

س (5): بين كيفية مساهمة إستراتيجية أمن المعلومات في تعزيز أمن المعلومات.

س (6): يؤكد المتخصصون على أن القوانين والتشريعات لا زالت عاجزة عن الحد من جرائم المعلومات، لماذا؟

س (7): يؤكد المتخصصون على حقيقة أنه لا قيمة لبرنامج أمن المعلومات مهما كانت التكنولوجيا المعتمدة فيها في حال فشل أو إخفاق الفراد العاملين في تطبيقه، هل أنت مع هذا التوجهأم لا ولماذا؟

س (8): يجب أن يبدأ الالتزام ببرنامج أمن المعلومات من الأفراد العاملين في المنظمة بدءاً من قمة الهرم وحتى قاعدته، كيف؟

س (9): ضع دائرة أمام الاجابة المناسبة.

يعد إدراك العاملين ومعرفتهم لأدوارهم ومسؤولياتهم في تطبيق برنامج أمن المعلومات في المنظمة:

A- غير مهمة ولا تاثير لهما	B- نصف المعركة في نجاح التطبيق
C- كامل المعركة في نجاح التطبيق	D- جميع ما ذكرغير صحيح

س (10): وضح باختصار اهم الاجراءات ذات العلاقة بالأفراد العاملين لتعزيز أمن المعلومات.

س (11): وضح باختصار اهم الاجراءات ذات العلاقة بأجهزة الفاكس لتعزيز أمن المعلومات.

س (12): وضح باختصار اهم الاجراءات ذات العلاقة بالتجسس وإنتحال الصفة لتعزيز أمن المعلومات.

س (13): ينصح المتخصصون عند استخدام كلمات السر (المرور) الالتزام ببعض القواعد، اذكر أهمها.

س (14): وضح باختصار اهم الاجراءات الاخرى ذات العلاقة بالملفات الالكترونية لتعزيز أمن المعلومات.

س (15): وضح باختصار اهم الاجراءات الخاصة لمواجهة الفايروسات لتعزيز أمن المعلومات.

س (16): وضح من خلال الشكل العمليات الرئيسة للتعامل مع أمن المعلومات في بيئة النظم.

س (17): يستخدم العديد من الشركات نظام تصنيف المعلومات للمساعدة في تأمين سرية وسلامة المعلومات، كيف ؟

س (18): وضح من خلال الشكل كيفية تصنيف المعلومات.

س (19): بصفتك متخصصاص في أمن المعلومات، بين كيف يسهم التوثيق في تعزيز أمن المعلومات؟

س (20): هناك عدد من الاجراءات الخاصة بتعزيز أمن المعلومات والتي تندرج في غطار تحديد المسؤوليات الادارية والشخصية، إشرحها بايجاز.

س (21): ما هو الهدف من إعتماد وسائل التعريف وصلاحية الاستخدام؟

س (22): يصنف الكتاب وسائل التعريف إلى ثلاثة أنواع، إشرحها بايجاز معززاً إجابتك بالشكل التوضيحي.

س (23): تكتسب سجلات الأداء(النفاذ) اهمية استثنائية في تعزيز امن المعلومات، لماذا؟ علل.

س (24): برأيك لماذا يجب أن تلجأ إدارة المنظمة إلى النسخ الاحتياطي؟

س (25): يؤكد المتخصصون على ضرورة وجود ثلاث وحدات تنظيمية لتولي مسؤولية أمن المعلومات في المنظمة، بين مسؤولية كل منها بأيجاز معززاً إجابتك بالشكل التوضيحي.

س (26): أجب بوضع إشارة (صح) أو إشارة (خطأ) أمام العبارات الآتية:

	العبارات	الاشارة
1	الحقيقة الجوهرية التي يجب الاعتراف بها هي: أن ما يجب القيام به لتعزيز الأمن هو معروف جيدا ولكن ليس جيدا بما فيه الكفاية.	
2	أجمع المتخصصون في هذا المجال حول طبيعة آلية تعزيز أمن المعلومات وأبعادها إلى الحد الذي يمكن معه الحديث عن أساليب معيارية موحدة يمكن اعتمادها من قبل مختلف المنظمات.	
3	يرى المتخصصون أن الاجراءات الخاصة بأمن المعلومات ذات العلاقة بالأفراد العاملين وصلت حد النضج والاكتمال.	
4	أن أفضل إجراء يمكن اعتماده لتجاوز الخروقات الأمنية في الهاتف النقال هو تجنب مناقشة الأمور الهامة والامتناع عن التحدث بالمعلومات الحساسة التي قد يؤدي تسريبها أو إساءة استخدامها إلى إلحاق الضرر بالمنظمة.	
5	الإجراءات الخاصة بمواجهة الفايروسات بحاجة إلى تحسين وتفعيلة مستمرين بسبب خطورة هذه الفيروسات وبسبب الأهداف التي تسعى إلى تحقيقها المتعاملون معها.	

الخاتمة

يبدو أن أمن المعلومات هي واحدة من القضايا التي لا يوجد لها حل ومواصلة ممارستها للتعبير عن المخاوف تم مناقشتها لسنوات عديدة، وهي:

- عدم وجود مقاييس كافية لوصف الأمن والمخاطر.
- سرعة الابتكار التقني الذي يفرض على الجميع، من الممارسين الى المستخدمين، ليكونوا في وضع التعلم واللحاق بالتطور.
- عواقب غير معروفة كونها المتبني الأول للتكنولوجيات المبتكرة.
- تحديات بناء الوعي حول كيفية الحفاظ على أمن بيانات المنظمة من قبل كل من الإدارة والقوى العاملة.
- مهارات الناس متنوعة (القراصنة) العازمين على الاحتيال والتجسس وسرقة الممتلكات الفكرية.
- النقص الواضح في الاهتمام بالموضوع الذي أبدته الإدارة العليا والمديرين التنفيذيين.
- البحث المستمر عن الموارد والتكنولوجيات الجديدة تجد طريقها إلى كل مجال من مجالات النشاط وتلعب دورا متزايد الأهمية.

سوف يتغير ذلك في المستقبل القريب ـ ربما، ولكن سيكون شيئا جيدا لو حصل هذا التغيير وكان هذا التغيير نحو الأفضل. انه لامر جيد ان نتذكر قصة من الأساطير اليونانية حول صندوق باندورا (Pandora's box). حيث تم إعلام (Pandora) صراحة من قبل (Zeus) بعدم فتح الصندوق ولكن (Pandora) فعل ذلك. وعندما قام بفتح الصندوق ، أطلق سراح كل

الشر في العالم قبل أن يتمكن من إغلاقه مرة أخرى وكان الشيء الوحيد الذي بقي في الصندوق هو "الأمل".

الأعمال الصغيرة ، على سبيل المثال، تحميل قطعة من البرمجيات لجهازحاسب شخصي ـ قد تبدو بسيطة وبريئة ولكنها قد تتحول إلى أن تكون له عواقب خطيرة. فهذه الامور يتعذر توفير المساعدة لها من قبل المجلات الشعبية لتكنولوجيا المعلومات والخاصة بالهواة والتي تشتمل على إرشادات ونصائح تفصيلية كاملة تتعلق بالبرمجيات، والأدوات والتعديلات على تكوين الأجهزة (مثل إجراء تغييرات على التسجيل) والتي قد تكون ملائمة للفرد ولكن تعد كارثية للمنظمة.

المراجع

أولاً: بالعربية

- المركز الوطني للتوثيق، أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها، متاح على الموقع الالكتروني: (http://www.arablaw.org).
- أسامة عبد الله قايد (1994):" الحماية الجنائية للحياة الخاصة وبنوك المعلومات "، دار النهضة العربية.
- ذياب البداينة (2002): الأمن وحرب المعلومات، دار الشروق، الاردن، عمان.
- حسن طاهر داود (2000): الحاسب وأمن المعلومات، السعودية، الرياض، معهد الادارة العامة.
- خضر مصباح الطيطي (2010): أساسيات امن المعلومات والحاسوب، دار الحامد للنشر والتوزيع، الاردن، عمان.
- ماجد عمار، "المسؤولية القانونية الناشئة عن استخدام فيروس الكومبيوتر " ، بحث مقدم إلى المؤتمر العلمي لنظم وتكنولوجيا المعلومات، القاهرة، (1990).
- محمد الهادي (2006): توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية، متاح في الموقع الالكتروني (http://www.journal.cybrains.info).

- محمد بن بلال القحطاني وخالد بن سليمان الغثبر (2009): أمن المعلومات بلغة ميسرة، السعودية، الرياض، مكتبة الملك فهد الوطنية.
- محمد سامي الشوا (1994) :"ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية.
- محمد عبد حسين الطائي، (2007):" نظام المعلومات الإدارية"، دار وائل للطباعة والنشر، عمان، الاردن.
- محمد عبد حسين، خضير نعمة عباس (2009):" نظم المعلومات الاستراتيجية"، دار الثقافة للنشر، عمان.
- هدى قشقوش (1992):"جرائم الحاسب الإلكتروني "، دار النهضة العربية.

ثانيا: بالأجنبية

- Altller, M. and Concepeion, (2000), Public Administration and Spatial Information (Unpublished lecture note).
- -A. Swanson,(1974) "Management Information System: Appreciation & Involvment,"(management Science,oct.,) ,pp.178-188.
- -American Accounting Association Committee on concepts and standard for exeternal financial reports(AAA;1977, pp13-16).

- -Ballou, D. P. and Pazer, H. L. ,(1985). Modeling data and process quality in multi-input, multi-output information systems. Management Science 31, 150-162
- Baruch Shapira (1993)."Ten Tips to Enhance Data Security " , Journal of Systems Management ,44 ,(June).
- -Belden Menkus (1990)."Celluar Telephone Use Can be Dangerous ", Modern Office Technology ,35 (August).
- -Belden Menkus (1993)."Laptop Security ", The Internal Auditor ,50 ,(February).
- -Brown, C. V., (1999), " Horizontal mechanisms under differing IS organization contexts". MIS Quarterly 23, 421-454.
- -Carolann Marine (1990)."The Spy Who Loves You ", Record Management Quarterly , 24(April) .
- Charles Cresson Wood &William W. Banks,Jr (1993)." Human Error: An Overlooked But Significant Information Security Ploblem,"Computers & Security,12 ,(February).
- -Cheney,P. & Dickson,G.B,(1982)," organizational characteristics and information system success; an Exploratory invistation,' Acd. Mgmt.J.Vol.25,No.1.

- Colin Richards-Carpenter (1993). "Keeping A system Safe & Secure ",Personnel Management ,(March).
- -Data Governance Star Wars: The Force of Agility,(2011) Information Management Blogs, June 9,. www.information-management.com.
- David C. Jones (1993)."Computer Advances Create New Data Theft Exposures", National Under Writer ,97,(June 14).
- -Donn B. Parker (1993). "A comprehensive List Of Threats To Information ", Information System Security,2ii,(Sumer).
- -Donn B. Parker(1997)."Information Security In A nutshell ", Information System Security, 6,(Spring).
- -Financial Accounting standards Board,(1977)"Expouser draft,Propose statement of financial accounting concepts,"(FASB, Dec, vol.29),p31.
- -Griffin, A. and Hauser, J. R., (1993)," The voice of customer". Marketing Science 12, 1-27.
- -Jane Griffin, Build a culture of accountability, Deloitte Consulting LLP (Information management,MAY-JUNE11, Info-mgmt.com).

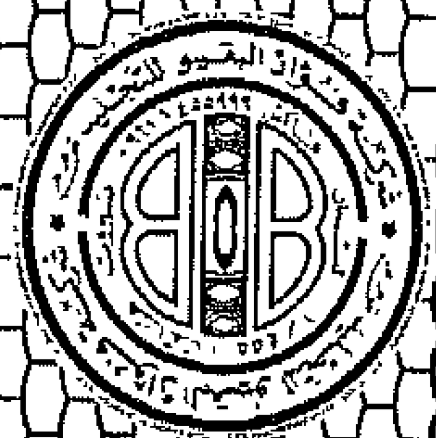
- Joe Abernathy (1991). "Former Hackers Offer Services in Computer Security", Houston Texas Chronicle,23,(June).
- -Lance J. Ewing , "Keeping the Lid on Secrets ", Risk Management , 39, (November1992).
- -Levitin, A. V. and Redman, T. C., ,(1998) Data as resource: Properties, implications, and prescriptions. Sloan Management Review, 89-101.
- -Lisa B. Hill," Information Security: An Overview & Resource Guide For Information Managers ",Record Management Quarterly ,29,(Jan1995) .
- -Lucas, H.C.(1990)"Information for management,"4th.ed.(McGrow-Hill,Inc.,).
- -Malcolm E. Palmer(2001). "Information Security Policy Framework" ,Information System Security ,10,(May-Jun).
- -Marc Tanzer (1993)." Keeping Spies Out of Your Company" , Personnel Journal , 72,(May)
- Michael Ley Zorek (1991). "A missing Feature in Some Records Management Systems", Records Management Quarterly,(January).
- -Olson, J. E.,(2003)," Data Quality: The Accuracy Dimension". Morgan Kaufmann, San Francisco, CA,.

- -O'Reilly,CH,(1982),"Variations in decision-maker's use of information sources,"Jour.Vol.25,No.4,.
- Patricia Graham Roy ,W.J. Kenny Jih & Ashok Roy (1991). "Computer Viruses:An Overview for Records Managers", Record Management Quarterly, 25,(April).
- Pfleeger, C. P. and Pfleeger, S. L.,(2003)," Security in computing". Prentice Hall, Upper Saddle River, NJ,.
- Pierre Van Beneden,(2011),"Information Governance: Records Management (Finally) Grows Up", KMWorld July/August.
- Rajn Chebiun (1991). "Computer Crimes: Passwords,Split Duties Safeguard Against Sabotage",Tallahassee Florida Democrat,6,(March,).
- Redman, T. C., (1998), The impact of poor data quality on the typical enterprise. Comm. ACM 41, 79-82.
- Singh, G., Bharathi, S., Chervenak, A., Deelman, E., Kesselman, C., Manohar, M., Patil, S., and Pearlman, L. A,(2003) metadata catalog service for data intensive applications. In Proceedings of the ACM/IEEE SC2003 Conference on High Performance Networking and Computing. (Phoenix, AZ,)

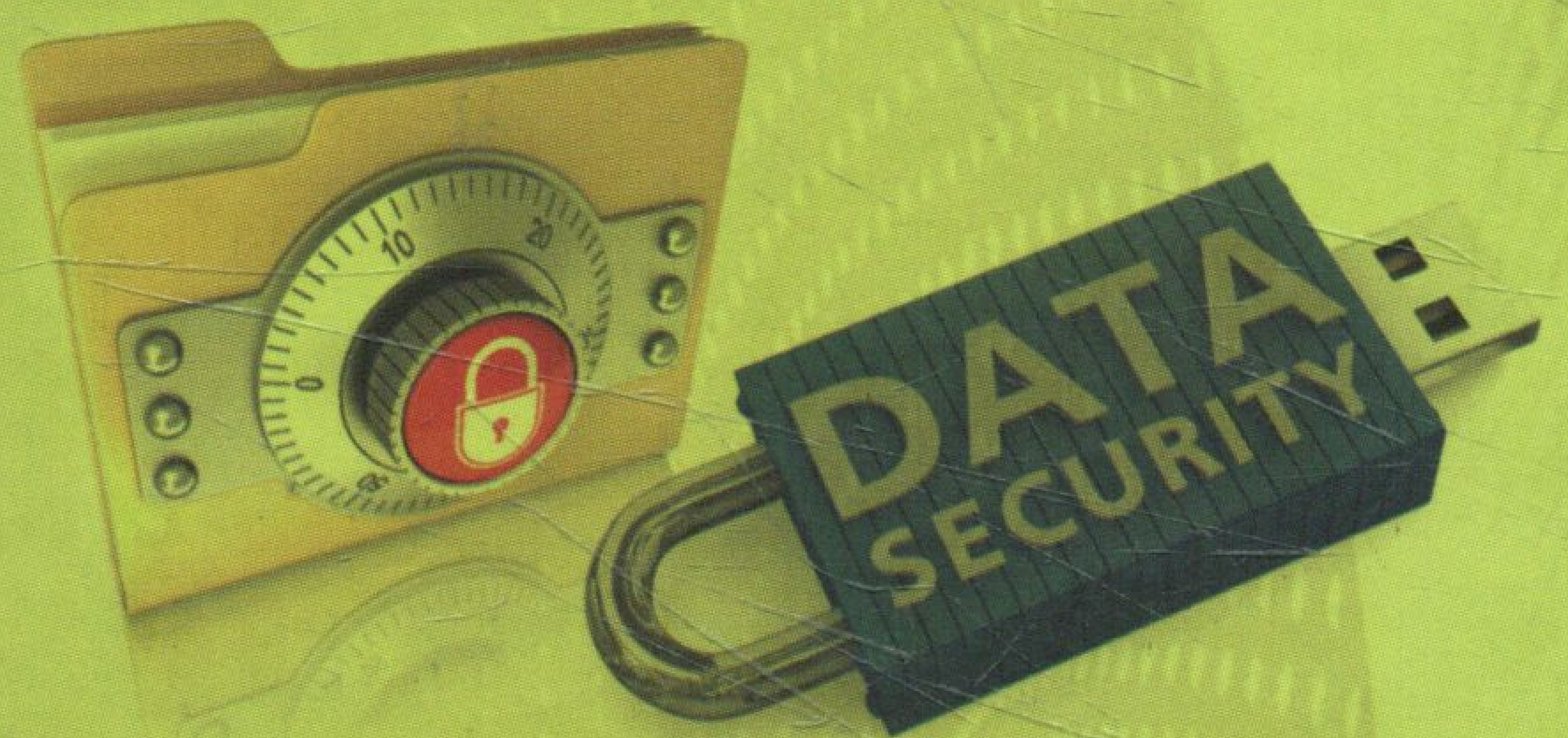
- -Stonebumber,G., Goguen, A., & Feringa,a.(2002). Risk management Guide for Information technology Systems,Nist special puplication,800(30).
- -Vijay Khatri and Carol V. Brown,(2011), Designing Data Governance, Organizations are becoming increasingly serious.
- -Wang, R. Y. and Strong, D. M. (1996), "Beyond accuracy: What data quality means to data consumers". Journal of Management Information Systems(12,, 5-34).
- Weill, P. and Ross, J. W.(2004)" IT governance: How top performers manage IT decision rights for superior results". Harvard Business School Press, Boston, MA.
- www.rsd.com,(2011)," Integrated Information Governance for Life Sciences: Protect Information Assets, Enable Defensible Disposition, and Harmonize Records Management.
- www.rsd.com, (2011)," Records Management is not Enough ,7 Reasons Why You Need Information Governance".







Information Security Management



Prof. Dr.
Mohammed A. H. Al-Taee

Dr.
M. Kilani

ISBN 978-9957-16-861-2



الثقافة للتصميم والإخراج



دار الثقافة للنشر والتوزيع

أسسها خالد محمود جبر حيف عام 1984 عمان - الأردن

Est. Khaled M. Jaber Haif 1984 Amman - Jordan

www.daralthaqafa.com